Elizabeth J. Cabraser (State Bar No. 083151)
Barry R. Himmelstein (State Bar No. 157736)
Michael W. Sobol (State Bar No. 194857)
Eric B. Fastiff (State Bar No. 182260)
Allison S. Elgart (State Bar No. 241901)
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008

Interim Class Counsel for MCI Class

Ronald L. Motley
Jodi W. Flowers
Donald A. Migliori
Justin B. Kaplan
Vincent I. Parrett (State Bar No. 237563)
MOTLEY RICE, LLC
28 Bridgeside Boulevard
P.O. Box 1792
Mount Pleasant, SC 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9440

Interim Class Counsel For Verizon Class

[Additional Counsel Appear On Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE: NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION, This Document Relates To: All Class Actions Against MCI and Verizon Defendants in the Master MCI and Verizon Consolidated Complaint, Dkt. 125	MDL No. 06-1791 VRW **PLAINTIFFS' JOINT OPPOSITION TO VERIZON'S MOTION TO DISMISS PLAINTIFFS' MASTER CONSOLIDATED COMPLAINT** Date: August 30, 2007 Time: 2:00 p.m. Courtroom: 6, 17th Floor Judge: Hon. Vaughn R. Walker

Dockets.Justia.com

TABLE OF CONTENTS

Page(s)

INTRODUCTION 1

PLAINTIFFS' CLAIMS 1

I. PLAINTIFFS HAVE SUFFICIENTLY ALLEGED INTERCEPTION AND DISCLOSURE OF THEIR COMMUNICATIONS AND RECORDS BY VERIZON.. 3

II. NO STATUTORY EXCEPTION JUSTIFIES DISMISSAL OF THOSE CLAIMS.. 4

A. The Master Complaint Alleges that Verizon Did Not Act Under Any Exception, and It Is Verizon's Burden to Prove Otherwise. 4

B. The Emergency Exception Cannot Be Fairly Read to Authorize the Alleged Disclosures. 7

C. The "Rights or Property" Exception Cannot Be Fairly Read to Authorize the Alleged Disclosures.. 9

III. THERE IS NO IMPLICIT EXCEPTION FOR CONDUCT RELATED TO FOREIGN INTELLIGENCE GATHERING JUSTIFYING DISMISSAL OF THOSE CLAIMS.. 11

A. There is No Implicit Exception to Title III 11

B. There is No Implicit Exception to ECPA.. 14

IV. THE AUMF DID NOT CREATE SUCH AN EXCEPTION.. 16

V. CLAIMS AGAINST VERIZON FOR INTERCEPTION AND DISCLOSURE DO NOT REQUIRE ALLEGATIONS OF HUMAN REVIEW BY NSA ANALYSTS.. 19

A. Claims of Interception Do Not Require Allegations of Human Review. 19

B. Claims Against Verizon for Disclosure of Plaintiffs' Communications and Records Do Not Require Allegations of Human Review by NSA Analysts, and Allegations that Verizon "Divulged," "Disclosed," "Provided" and/or "Provided Access To" Plaintiffs' Communications and Records Are More Than Sufficient...... 21

VI. PLAINTIFFS' CLAIMS FOR VIOLATIONS OF ECPA DO NOT RUN AFOUL OF THE FIRST AMENDMENT.. 24

TABLE OF CONTENTS
(continued)

Page(s)

A. If Accepted, Verizon's Argument Would Eviscerate a Broad Swath of Non-Disclosure Laws and Statutory Duties of Confidentiality. 25

B. ECPA's Customer Record Provisions Are Content Neutral, Because They Further the Content Neutral Purpose of Promoting Customer Privacy and Private Speech. 27

C. Even If ECPA Is Treated as a Content Based Restriction on Speech, Application of ECPA to Verizon's Massive Disclosure of Customer Records Is Subject to a Balancing Test, or at Most Intermediate Scrutiny. 30

1. The Customer Records Non-Disclosure Provisions of ECPA Further Privacy, Which In Turn Fosters Private Speech, Both of Which Are Interests of the Highest Order. 30

2. In Cases Involving Competing Interests in Speech, On the One Hand, and Privacy Which Fosters Private Speech, On the Other, Strict Scrutiny Does Not Apply Where the Disclosure Bar Applies to Speech That is Not of Public Concern. 32

3. The Disclosure of Verizon's Customer Records Is Not Speech on a Matter of Public Concern. 34

D. Under Either a Balancing Inquiry or Intermediate Scrutiny, The Application of ECPA to Verizon's Disclosure of Its Customers' Phone Records Is Permissible. 35

1. The Interest in Protecting Privacy and Fostering Private Speech Far Outweighs Verizon's Asserted Interest In Turning Over the Records of Millions of Customers to the Government 35

2. Application of ECPA to Verizon's Disclosure of the Records of Millions of Its Customers Easily Satisfies Intermediate Scrutiny. 38

E. The Petition Clause Does Not Immunize Verizon's Disclosure of Its Customer Records to the Federal Government. 40

F. The Doctrine of Constitutional Avoidance Does Not Require That The Court Rewrite ECPA. 45

TABLE OF CONTENTS
(continued)

Page(s)

VII. PLAINTIFFS' STATE LAW CLAIMS ARE WELL PLEADED, AND VERIZON'S SWEEPING PREEMPTION THEORIES ARE UNFOUNDED. 45

A. Federal Law Does Not Preempt Plaintiffs' State Law Claims. 45

B. Plaintiffs' State Law Claims Satisfy Notice Pleading Standards. 47

VIII. THE CLAIMS AGAINST MCI ARE NOT BARRED BY MCI'S BANKRUPTCY DISCHARGE. 49

CONCLUSION 53

TABLE OF AUTHORITIES

Page

CASES

ACLU v. Nat'l Sec. Agency/Central Sec. Serv., 438 F. Supp. 2d 754 (D. Mich. 2006) 17

Acorn v. City of Phoenix, 798 F.2d 1260 (9th Cir. 1986) 28

Aguilar v. United States, 515 U.S. 593 (1995) 37

American Motors Corp. v. Huffstutler, 575 N.E.2d 116 (Ohio 1991) 37

Andresen v. Maryland, 427 U.S. 463 (1976) 24

Apple v. Glenn, 183 F.3d 477 (6th Cir. 1999) 41

Bartnicki v. Vopper, 532 U.S. 514 (2001) .... passim

BE & K Const. Co v. NLRB, 536 U.S. 516 (2002) 42, 43

Berger v. New York, 388 U.S. 41 (1967) 24

Bicoastal Corp. v. Aetna Cas. And Sur. Co., No. C-94-20108, 1994 WL 564539 (N.D. Cal. Oct. 4, 1994) 48

Brown v. Continental Telephone Company of Virginia, 670 F.2d 1364 (4th Cir. 1982) 13

Bubis v. United States, 384 F.2d 643 (9th Cir. 1967) 9, 10

California Motor Transport Co. v. Trucking Unlimited, 404 U.S. 508 (1972) 41

Carroll v. United States, 267 U.S. 132 (1925) 36

Casey v. United States, 191 F.2d 1, 4 (9th Cir. 1951) 9

Chaganti v. 12 Phone Int'l Inc., No. 04-CV-0987, 2005 WL 679664 (N.D. Cal. March 11, 2005) 47

Chapman v. Houston Welfare Rights Organization, 441 U.S. 600 (1979) 44

City of Indianapolis v. Edmond, 531 U.S. 32 (2000) 37

Cohen v. Cowles Media, 501 U.S. 663 (1991) 27

Connick v. Myers, 461 U.S. 138 (1983) 34

Page

Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985) 34, 35

DVD Copy Control Assn., Inc. v. Bunner, 31 Cal.4th 864 (Cal. 2003) 32, 35, 36

Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004) 48

Eastern R. R. Presidents Conference v. Noerr Motor Freight, Inc., 365 U.S. 127 (1961) 41

Edmond v. U.S., 520 U.S. 651 (1997) 17

English v. General Elec. Co., 496 U.S. 72 (1990) 46

Expo Chemical Co. v. Brooks, 572 S.W.2d 8 (Tex. Civ. App. 1978) 27

Florida Star v. B.J.F., 491 U.S. 524 (1989) .... passim

Forro Precision, Inc. v. IBM Corp, 673 F.2d 1045 (9th Cir. 1982) 42

Freedman v. America Online, Inc., 303 F. Supp. 2d 121 (D. Conn. 2004) 7

Hamdan v. Rumsfeld, 126 S. Ct. 2749 (2006) 17, 18

Hamdi v. Rumsfeld, 542 U.S. 507 (2004) 18

Hill v. Colorado, 530 U.S. 703 (2000) 28, 29

Hodge v. Mountain States Telephone and Telegraph Company, 555 F.2d 254 (9th Cir. 1977) 10

In re Application of U.S. for Nunc Pro Tunc Order for Disclosure of Telecommunications Records, 352 F. Supp. 2d 45 (D. Mass. 2005) 8

In re Chemetron Corp., 72 F.3d 341 (3rd Cir. 1995) 50

In re Conseco Life Ins. Co. Cost of Insurance Litigation, 2005 WL 2203150 (C.D. Cal. 2005) 50, 52

In re Emelity, 251 B.R. 151 (Bankr. S.D. Cal. 2000) 52

In re Hassanally, 208 B.R. 46 (9th Cir. BAP 1997) 52

In re Hexcel Corp., 239 B.R. 564 (N.D. Cal. 1999 .... 50, 52

In re Jensen,

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
ATTORNEYS AT LAW
SAN FRANCISCO

TABLE OF AUTHORITIES
(continued)

Page

995 F. 2d 925 (9th Cir. 1999) ... 50, 51

In re Maya Construction Company, 78 F.3d 1395 (9th Cir. 1996) ... 50

In re NSA Telecoms. Records Litig., MDL No. 06-1791, 2007 U.S. Dist. LEXIS 3786, 2007 WL 163106 (N.D. Cal. Jan. 18, 2007) ... 46

In re Quarles, 158 U.S. 532 (1895) ... 42, 44

In re Russell, 193 B.R. 568 (Bankr. S.D. Cal. 1996) ... 52

In re Sacred Heart Hosp., 133 F.3d 237 (3d Cir. 1998) ... 44

In re Savage Industries, Inc., 43 F. 3d 714 (1st Cir. 1994) ... 50

In re Worldcom, Inc., 320 B.R. 772 (Bankr. S.D.N.Y. 2005) ... 52

In re Worldcom, Inc., 328 B.R. 35 (Bankr. S.D.N.Y. 2005) ... 52

In re XO Communications, 301 B.R. 782 (Bankr. S.D.N.Y. 2003) ... 50

Jacobson v. Rose, 592 F.2d 515 (9th Cir. 1978) ... 4

King v. Idaho Funeral Serv. Ass'n, 862 F.2d 744 (9th Cir. 1988) ... 42

Kottle v. Northwest Kidney Centers, 146 F.3d 1056 (9th Cir. 1998) ... 43, 44

Leatherman v. Tarrant County Narcotics Intelligence & Coordination Unit, 507 U.S. 163 (1993) ... 4

McClelland v. McGrath, 31 F. Supp. 2d 616 (N.D. Ill. 1998) ... 10

McDonald v. Smith, 472 U.S. 479 (1985) ... 42

McIntyre v. Ohio Elections, Com'n, 514 U.S. 334 (1995) ... 31

Monster Content, LLC v. Homes.Com, Inc., 331 B.R. 438 (N.D. Cal. 2005) ... 50

Morales v. TWA, Inc., 504 U.S. 374 (1992) ... 17

NAACP v. Alabama, 357 U.S. 449 (1958) ... 31

Northwest Pipe Co. v. Travelers Indem. Co., No. 02-CV-04189, 2003 U.S. Dist. LEXIS 26416, 2003 WL 24027882 (N.D.

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
ATTORNEYS AT LAW
SAN FRANCISCO

TABLE OF AUTHORITIES
(continued)

Page

Cal. Feb. 12, 2003) 48

O'Loghlin v. County of Orange, 229 F.3d 871 (9th Cir. 2000) 51

Olmstead v. United States, 277 U.S. 438 (1928) 31

Payton v. New York, 445 U.S. 573 (1980) 24, 36

Rendish v. City of Tacoma, 123 F.3d 1216 (9th Cir. 1997) 42

Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994) 20

Shulman v. Group W Productions, 18 Cal. 4th 200, 74 Cal. Rptr. 2d 843 (1998) 23

Smith v. Arkansas State Highway Emp., Local 1315, 441 U.S. 463 (1979) 41

Sosa v. DIRECTV, Inc., 437 F.3d 923 (9th Cir. 2006) 42, 43

Sure-Tan, Inc. v. NLRB, 467 U.S. 883 (1984) 44

Trans Union v. Federal Trade Commission, 245 F.3d 809 (D.C. Cir. 2001) 35, 38, 39

Trans Union v. FTC (*Trans Union II*), 267 F.3d 1138 (D.C. Cir. 2001) 38, 39

Turner Broadcasting, Inc. v. FCC, 512 U.S. 622 (1994) 28, 29, 38

U.S. v. Capra, 501 F.2d 267 (2d Cir. 1974) 8

U.S. v. Crouch, 666 F. Supp. 1414 (N.D. Cal. 1987) 8

U.S. v. First City Nat'l. Bank of Houston, 386 U.S. 361 (1967) 5

U.S. v. Goldstein, 532 F.2d 1305 (9th Cir. 1976) 6, 10

U.S. v. Koyomejian, 970 F.2d 536 (9th Cir. 1992) 12

U.S. v. Rodriguez, 968 F.2d 130 (2d Cir. 1992) 19

U.S. v. Torres, 751 F.2d 875 (7th Cir. 1985) 12

United States v. Barnard, 490 F.2d 907 (9th Cir. 1973) 13

TABLE OF AUTHORITIES
(continued)

Page

United States v. Beckley, 259 F. Supp. 567 (N.D. Ga. 1965) 9

United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982) 12

United States v. Kokinda, 497 U.S. 720 (1990) 28

United States v. Playboy Entm't Group, Inc., 529 U.S. 803 (2000) 32

United States v. Ron Pair Enterprises, Inc., 489 U.S. 235 (1989) 16

United States v. Smith, 155 F.3d 1051 (9th Cir. 1998) 21

United States. v. Oakland Cannabis Buyers' Co-op, 532 U.S. 483 (2001) 45

Venture Assoc. Corp. v. Zenith Data Systems Corp., 987 F.2d 429 (7th Cir. 1993) 48

W. Va. Univ. Hosps. V. Casey, 499 U.S. 83 (1991) 16

Ward v. Rock Against Racism, 491 U.S. 781 (1989) 28, 29

Wayte v. United States, 470 U.S. 598 (1985) 42

West v. Worldcom, Inc., 2007 WL 485233 (S.D.N.Y. 2007) 52

Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952) 18

STATUTES

12 U.S.C. § 340 25

12 U.S.C. § 3402 25

15 U.S.C. § 1681 26

15 U.S.C. 77s(c) 40

18 U.S.C. § 2510(19) 16

18 U.S.C. § 2511 32

18 U.S.C. § 2511(1) 11, 12

18 U.S.C. § 2511(2) 12

18 U.S.C. § 2511(2)(a)(i) 9

18 U.S.C. § 2511(2)(a)(ii) 14

18 U.S.C. § 2511(2)(e) 13

TABLE OF AUTHORITIES
(continued)

Page

18 U.S.C. § 2511(2)(f) 11, 13, 16
18 U.S.C. § 2511(3) 12, 13
18 U.S.C. § 2511(c) 32
18 U.S.C. § 2516 12
18 U.S.C. § 2518 12
18 U.S.C. § 2518(7) 8
18 U.S.C. § 2520 14
18 U.S.C. § 2701 .... 20, 21
18 U.S.C. § 2702 .... 21, 22
18 U.S.C. § 2702(a) 21
18 U.S.C. § 2702(a)(3) 15
18 U.S.C. § 2702(b)(7) 15
18 U.S.C. § 2702(c) 6, 41, 43
18 U.S.C. § 2702(c)(3) 4, 9, 10, 15
18 U.S.C. § 2702(c)(4) 4, 7, 9, 15
18 U.S.C. § 2702(c)(5) 40
18 U.S.C. § 2703 7
18 U.S.C. § 2703(c)(2) 40
18 U.S.C. § 2707(e) 5, 15
18 U.S.C. § 2709 15
18 U.S.C. 2511(c) 32
18 U.S.C. § 2703(c)(4) 6
20 U.S.C. § 1232g(b) 26
42 U.S.C. § 13032 40
42 U.S.C. § 13032(b) 40
42 U.S.C. § 1320d-6 26
47 U.S.C. § 222(c) 39
47 U.S.C. § 605 .... 9, 13
50 U.S.C. § 1801 15
50 U.S.C. § 1801(e) (2006) 14
50 U.S.C. § 1810 14
50 U.S.C. § 1861 16
50 U.S.C.A. § 1541 17
115 Stat. 1394, § 314(a)(2)(B) (Dec. 28, 2001) 17
115 Stat. 272, §§ 206-108, 214-218, 504, 1003 17

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
ATTORNEYS AT LAW
SAN FRANCISCO

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
ATTORNEYS AT LAW
SAN FRANCISCO

TABLE OF AUTHORITIES
(continued)

Page

Pub. L. No. 95-511, § 201(c) 13

Pub. L. No. 99-508 15

Act of June 19, 1968, Pub. L. No. 90-351, § 2511, 82 Stat. 197, 214 12

Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (Sept. 18, 2001) 17

UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 433 (1985) 27

USA PATRIOT Improvement and Reauthorization Act ("PATRIOT Reauthorization Act"), Pub. L. No. 109-177, Title I, § 107(b)(1)(B), 120 Stat. 192, 202 (Mar. 9, 2006) 6

RULES

Federal Rules of Civil Procedure Rule 8(c) 50

TREATISES

Rest. (2d) Torts § 139(2) 44

Rest. (2d) Torts, § 652B 24

CONSTITUTIONAL PROVISIONS

U.S. Const., Am. I 41

OTHER AUTHORITIES

147 Cong. Rec. S. 10365, 10371 10

147 Cong. Rec. S10365-02 (Oct. 26, 2001) 6

1978 U.S.C.C.A.N. 3910 13

1986 U.S.C.C.A.N. 2112, 2182 10

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev.1083 (2002) 40

Daniel J. Solove, *The First Amendment as Criminal Procedure,* 82 N.Y.U. L. Rev. 112, 1123 (2007) 31

H.R. Rep. No. 95-1283 14

H.R.Rep. No. 99-647 (1986) 23, 30

Neil M. Richards, *Reconciling Data Privacy and The First Amendment,* 52 UCLA L. Rev. 1149 (2005) 27

Office of Technology Assessment , *Electronic Surveillance and Civil Liberties* 36

President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967) 31

TABLE OF AUTHORITIES
(continued)

Page

Richards, *Reconciling Data Privacy*, 52 UCLA L. Rev. at 1158 38

Rodney Smolla, *Information as Contraband*: *The First Amendment and Liability for Trafficking in Speech*, 96 Nw. U. L. Rev. 1099, 1130 (2002) 31

S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555 .... 24, 29, 30, 40

S. Rep. No. 95-604(I) 12, 13

S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., S. Rep. No. 94-755 (1976) (Church Committee Books I-VI) 12

Testimony of Kris Anne Montieth, Chief, Enforcement Bureau, FCC. Hearing on "Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?" Sub-Committee on Oversight and Investigations. Committee on Energy and Commerce. U.S. House of Representatives. September 26, 2006 31

Tom Daschle, *Power We Didn't Grant*, WASH. POST, Dec. 23, 2005, at A21 18

Wartime Executive Power and the NSA's Surveillance Authority (Part I): Hearing Before the Senate Judiciary Committee, 109th Cong., at 186 (2006) 17

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
ATTORNEYS AT LAW
SAN FRANCISCO

INTRODUCTION

In addition to rehashing the government's state secrecy arguments, which are addressed in the companion brief filed herewith,[1] Verizon[2] makes three major arguments for the threshold dismissal of this case. These arguments strain statutory interpretation, constitutional law, and common sense all to the breaking point.

First, Verizon argues that the narrow statutory exceptions for emergencies and protection of its own networks at 18 U.S.C. § 2702(c) immunize it from liability for the ongoing, wholesale disclosure of millions of its customers' communications records to the government for a period of over 5 years (and counting). Second, Verizon urges this Court to imply a new "government says national security" exception into all of the nations' surveillance laws, or read one into the Authorization for Use of Military Force, Pub. L. No. 107-40 ("AUMF"). Finally, Verizon urges this Court to make a breathtaking ruling that the nations' privacy laws violate the First Amendment and so cannot be applied to protect Verizon's customers from the wholesale disclosure of their communications records to the government. None of these novel arguments should succeed. To the contrary, this case should proceed to discovery and trial, so that the ongoing illegal surveillance of millions of innocent Americans may finally be ended.

PLAINTIFFS' CLAIMS

Like the *Hepting* complaint, the Master Complaint asserts federal constitutional and statutory claims for violations of:

> (1) The First and Fourth Amendments to the United States Constitution (acting as agents or instruments of the government) by illegally intercepting, disclosing, divulging and/or using plaintiffs' communications [Sixth Claim for Relief];

---

[1] To avoid unnecessary repetition, Plaintiffs incorporate by reference The Factual Background section of the accompanying Plaintiffs' Joint Opposition to Motion to Dismiss or, in the Alternative, For Summary Judgment By The United States of America and to State Secrets and Related Arguments In Verizon's Motions to Dismiss. As the title indicates, Plaintiffs also respond to Verizon's arguments regarding the state secrets privilege in the accompanying brief.

[2] For simplicity, unless otherwise indicated, the defendants named in the Master Consolidated Complaint Against MCI Defendants and Verizon Defendants ("Master Complaint," Dkt. No. 125) will be referred to collectively as "Verizon" or "Defendants," and the plaintiffs in the Master Complaint will be referred to collectively as "Plaintiffs."

(2) Section 109 of Title I of the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1809, by engaging in illegal electronic surveillance of plaintiffs' communications under color of law [Fifth Claim for Relief];

(3) Section 802 of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by section 101 of Title I of the Electronic Communications Privacy Act of 1986 (ECPA) ["Title III"], 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d) and (3)(a), by illegally intercepting, disclosing, using and/or divulging plaintiffs' communications [Third Claim for Relief];

(4) Section 705 of Title VII of the Communications Act of 1934, as amended, 47 U.S.C. § 605, by unauthorized divulgence and/or publication of plaintiffs' communications [Fourth Claim for Relief];

(5) Section 201 of Title II of the ECPA ("Stored Communications Act"), as amended, 18 U.S.C. §§ 2702(a)(1) and (a)(2) ["ECPA"], by illegally divulging the contents of plaintiffs' communications [First Claim for Relief];

(6) Section 201 of the Stored Communications Act, as amended by section 212 of Title II of the USA PATRIOT Act, 18 U.S.C. § 2702(a)(3) ["ECPA"], by illegally divulging records concerning plaintiffs' communications to a governmental entity [Second Claim for Relief;] and

(7) California's Unfair Competition Law, Cal Bus & Prof Code §§ 17200 et seq., by engaging in unfair, unlawful and deceptive business practices [Tenth Claim for Relief].

Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978-79 (N.D. Cal. 2006) (listing claims asserted in *Hepting*).

The Master Complaint also asserts several claims for relief arising under state law, specifically: (1) violation of the surveillance statutes of all States and the District of Columbia (Seventh Claim for Relief); (2) violation of the consumer protection statutes of all States and the District of Columbia, based, *inter alia*, on Defendants' violation of their own privacy policies, which falsely assured customers that Defendants would not divulge their customers' communications or records except as required by law (Eighth Claim for Relief); and (3) common law breach of contract, based on the violation of Defendants' privacy policies (Ninth Claim for Relief).

In sum, Plaintiffs allege Verizon's wholesale interception and disclosure of their communications and records, for and to the government.

I. PLAINTIFFS HAVE SUFFICIENTLY ALLEGED INTERCEPTION AND DISCLOSURE OF THEIR COMMUNICATIONS AND RECORDS BY VERIZON.

Verizon claims that Plaintiffs have failed to sufficiently plead the interception and disclosure of Plaintiffs' records and communications to the government, because they have not alleged that NSA analysts chose to target Plaintiffs' information for personal review after obtaining it from Verizon. Memorandum in Support of Verizon's Motion to Dismiss Plaintiffs' Master Consolidated Complaint ("Ver. Mem.") at 9-10 (interception), 23-26 (disclosure). This claim is incorrect; indeed, this Court has already ruled on a similar question in regard to AT&T's alleged communications dragnet. In *Hepting*, the Court correctly recognized that the plaintiffs' claims did not rely on the means or methods of the government's program, but instead "focuse[d] only on whether AT & T intercepted and disclosed communications or communication records to the government," and that "plaintiffs need not allege any facts regarding the government's conduct to state these claims." 439 F. Supp. 2d at 994, 999.

The same is true here. Putting aside Verizon's word-games and absurd resort to the common law of defamation, Plaintiffs have plainly alleged Verizon's interception of Plaintiffs' communications for the government,[3] and the disclosure or "divulgence" of those communications and Plaintiffs' records to the government.[4] These plain allegations are more than sufficient under notice pleading standards.

---

[3] *See, e.g.*, Master Consolidated Complaint Against MCI Defendants and Verizon Defendants ("Master Complaint," or "MCC") ¶¶ 245 ("Verizon ha[s] intentionally acquired, by means of a surveillance device, the contents of one or more wire communications to or from Plaintiffs and class members") and 231 (Verizon has intentionally intercept[ed]" the contents of telephone calls of [its] customers," including Plaintiffs, *see id.* at ¶ 233); *see also* MCC ¶ 168 ("Defendants have intercepted and continue to provide the government with direct access to all or a substantial number of the communications transmitted through their key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and electronic communications.").

Plaintiffs have alternatively alleged that Verizon assisted the government in conducting the interceptions, rather than acquiring the communications itself. *See id.* at ¶ 175 ("Using [surveillance] devices, government agents have acquired and are acquiring wire or electronic communications content . . . and/or Defendants [have] disclosed and are disclosing those communications . . . after interception . . . ."); *see also id.* at 173-175 (alleging that Verizon authorized and assisted in the installation and use of the "interception devices" in its facilities, devices which "capture[d] [or] record[ed] . . . all or a substantial number" of the communications transmitted through those facilities).

II. NO STATUTORY EXCEPTION JUSTIFIES DISMISSAL OF THOSE CLAIMS.

A. The Master Complaint Alleges that Verizon Did Not Act Under Any Exception, and It Is Verizon's Burden to Prove Otherwise.

As it must for purposes of its motion to dismiss, Verizon accepts the allegations in the Master Complaint as true (Ver. Mem. at 2),[5] and those allegations definitively foreclose Verizon's attempt to justify its years-long, massive disclosure of its customers' records based on the statutory exceptions allowing disclosure in emergency situations (18 U.S.C. § 2702(c)(4)) or as necessary to protect Verizon's "rights or property" (18 U.S.C. § 2702(c)(3)). Ver. Mem. at 20-22, 26, 44-46. The Master Complaint plainly alleges that in disclosing its customers' records to the government, Verizon acted "without . . . statutory authorization . . . pursuant to Chapters 119 and 121 of Title 18 of the United States Code," and without any "other lawful authorization."

Such assistance is more than sufficient to establish Plaintiffs' claims. *See Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) ("Because [the phone company] joined with the [government agents] in the wiretapping, its failure to listen to the tapes should not insulate it from liability . . . .), *citing White v. Weiss*, 535 F.2d 1067, 1071 (8th Cir. 1976) (holding that conduct of private detective who personally assisted a wife's installation of a phone wiretap to monitor her husband constituted an interception, even though it was the wife who personally hooked up the equipment and monitored the phone conversations).

[4] *See, e.g.*, MCC ¶¶ 169 ("Since in or about October 2001 . . . Verizon ha[s] disclosed and/or divulged the 'call-detail records' of all or substantially all of their customers, including Plaintiffs, to the NSA"); ¶ 171 ("Defendants have disclosed and continue to disclose . . . their databases of stored telephone and electronic communications records"); ¶ 175 ("Verizon ha[s] disclosed and [is] disclosing communications and information to the government after interception"); ¶ 218 ("Defendants violated 18 U.S.C. § 2702(a)(3) by knowingly and intentionally divulging to the federal government records or other information pertaining to subscribers or customers of Defendants' remote computing and electronic service(s)," including Plaintiffs, *see id.* at ¶ 226 ("Plaintiffs . . . are aggrieved by . . . Verizon's knowing and intentional past disclosure and/or imminent future disclosure of their records to the federal government)); 230 ("Verizon violated 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a) by intentionally intercepting and disclosing to the federal government the contents of telephone calls of [its] customers," including Plaintiffs, *see id*. at ¶ 233 ("Plaintiffs . . . are aggrieved by Defendants' intentional past and/or imminent future interception and disclosure of telephone call contents to the federal government")); and ¶ 247 ("Defendants have intentionally disclosed . . . information obtained under color of law by electronic surveillance," including Plaintiffs' communications, *see id.* at ¶ 246).

[5] On a motion to dismiss, the Court "must accept as true all the factual allegations in the complaint." *Leatherman v. Tarrant County Narcotics Intelligence & Coordination Unit*, 507 U.S. 163, 164 (1993).

MCC ¶ 177; *see also id.* at ¶ 225 (Verizon's disclosures of records "were and are not authorized by any statute . . . .").[6]

Although these general allegations are sufficient to dispose of the issue on motion to dismiss (*see Hepting*, 439 F. Supp. 2d at 1002-03), the Master Complaint also *specifically* alleges that Verizon's records disclosures "were not [made] . . . to protect the rights or property of Defendants," nor "based on a reasonable and/or good faith belief that an emergency involving danger of death or serious physical injury required disclosure without delay . . . ." MCC ¶ 182. Indeed, the Master Complaint alleges that Verizon engaged in this conduct "with knowledge of [its] illegality, and therefore in bad faith." MCC ¶ 183. Acceptance of these allegations as true forecloses any possibility that Verizon may obtain dismissal by relying on those exceptions, particularly considering that statutory authorizations provide a defense only when relied upon in good faith. 18 U.S.C. § 2707(e).

Of course, Plaintiffs did not need to plead affirmatively Verizon's failure to rely on the exceptions to avoid dismissal, since ECPA—like Title III—contains no heightened pleading requirement. *See Hepting*, 439 F. Supp. 2d at 1002 (noting lack of heightened pleading requirement in Title III). Rather, it is Verizon's responsibility to prove that the exceptions apply, pursuant to the well-established principle of statutory construction holding that the party seeking the benefit of an exception to a statutory prohibition bears the burden of proof. *See U.S. v. First City Nat'l. Bank of Houston*, 386 U.S. 361, 366 (1967). In the face of such precedent, Verizon tries to raise the specter of a "factually intensive" and "protracted" inquiry into its state of mind in order to avoid directly stating its actual argument: that it can avail itself of the exceptions without offering *any proof at all*. Ver. Mem. at 21-22.

Such an overreaching position simply cannot be squared with the statute's plain language, which Verizon notably fails to state. To avail itself of the emergency exception at 18 U.S.C. § 2702(c)(4), as amended in 2006, Verizon must prove that it had a "good faith[ ]belie[f]" that its disclosure was justified by an emergency, that the emergency required action "without delay," and that its disclosure was limited to records that actually "relat[ed] to the emergency." *See* USA PATRIOT Improvement and Reauthorization Act ("PATRIOT Reauthorization Act"), Pub. L. No. 109-177, Title I, § 107(b)(1)(B), 120 Stat. 192, 202 (Mar. 9, 2006).

---

[6] Notably, Verizon itself characterizes both of the relevant exceptions as "statutory authorization[s]". Ver. Mem. at 46; *see also In re Application of U.S. for Nunc Pro Tunc Order for Disclosure of Telecommunications Records*, 352 F. Supp. 2d 45, 47 (D. Mass. 2005) (characterizing emergency exception as a "statutory authorization").

As for its conduct prior to 2006, Verizon must further prove that its belief in an "immediate" emergency was "reasonabl[e]" in order to benefit from the emergency exception as originally codified in 2001. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("PATRIOT Act"), 147 Cong. Rec. S10365-02 (Oct. 26, 2001) (codified as amended at 18 U.S.C. § 2702(c)) (exception allows disclosure "to a governmental entity, if the provider *reasonably* believes that an emergency involving *immediate* danger of death or serious physical injury to any person justifies disclosure of the information" (emphasis added)).[7]

Similarly, to benefit from the "rights or property" exception also codified at 18 U.S.C. § 2702(c), Verizon must prove that its disclosures were "*necessarily* incident" to protecting its rights or property, *id.* at § 2703(c)(4) (emphasis added), and courts have consistently interpreted that language to require a demonstration of the *reasonableness* of Verizon's conduct. *See, e.g., U.S. v. Goldstein*, 532 F.2d 1305, 1311-12 (9th Cir. 1976) (in applying identical "rights or property" exception in Title III, holding that communications provider's conduct must be reasonable).[8]

Indeed, a brief look at the case law construing these exceptions demonstrates how demanding these requirements are, and shows the manifest unreasonableness of Verizon's position.

---

[7] Because this original formulation applies to most of the period covered by the Master Complaint, and—unlike the amended exception's language—it has been previously considered by the courts, Plaintiffs' discussion will focus on it. However, and as further discussed below, the 2006 amendment does little to bolster Verizon's argument, and in fact weakens it.

[8] The requirements of the "rights or property" exception are discussed at length *infra*, at pp. 9-11.

B. The Emergency Exception Cannot Be Fairly Read to Authorize the Alleged Disclosures.

Only one court has considered 18 U.S.C. § 2702(c)(4)'s exception for emergency records disclosure at any length. That court, in declining to apply the exception, reached the only conclusion that the plain language of the exception allows: that the emergency exception is reserved for voluntary disclosures in response to specific and urgent emergencies, and that it is the burden of the defendant to prove the exception's applicability. *See Freedman v. America Online, Inc.*, 303 F. Supp. 2d 121, 127-28 (D. Conn. 2004).

In *Freedman*, the plaintiff argued that the defendants—two police officers—had violated ECPA by soliciting from America Online ("AOL") the disclosure of his subscriber information based on an unsigned warrant application, rather than following the procedures provided in 18 U.S.C. § 2703 for obtaining such information. *See id.* at 122-23. The defendants sought this information because the plaintiff had sent an email concerning a political campaign that stated "The End is Near," and two recipients had reported the email to the police as "harassing and/or obscene." *Id.* at 123 n.4. In response to the plaintiff's motion for partial summary judgment, the defendants contended, *inter alia*, that there was a genuine issue of material fact as to whether AOL disclosed the information pursuant to the emergency exception at 18 U.S.C. § 2702(c)(4), arguing that the exception did not prohibit disclosures based on government requests.

The court flatly rejected the defendants' argument, in a passage worth quoting at length:

> Defendants' argument is flawed. First, their conclusory speculation about what AOL "may have believed" is not only lacking in any evidentiary substantiation, but it is also insufficient to raise a genuine issue of material fact to survive summary judgment. They offer no evidence from which a reasonable juror could conclude that AOL believed the e-mail recipients were in immediate danger. Second, as Plaintiff notes, it took AOL over six days to respond to the officers' request for information, a delayed response which severely undermines Defendants' conclusory allegation that AOL "may have believed" the e-mail recipients were in immediate danger. Under the circumstances of this case, Defendants fail to raise a genuine issue of material fact whether AOL disclosed Plaintiff's subscriber information pursuant to the ECPA emergency disclosure exception. The government may not circumvent the legal process specified in the ECPA pursuant to the "emergency" exception on such a speculative basis.

Id. at 127-28 (internal citations omitted). To benefit from the emergency exception, it is Verizon's burden to offer evidence that it *actually believed* that a threat of immediate danger to certain individuals justified its disclosure. Conclusory speculation about what Verizon may have believed cannot justify the government's circumvention of the legal process required under 18 U.S.C. § 2703. *See Freedman*, 303 F. Supp. 2d at 127-28.

Such generalized fears are not sufficient to support a reasonable or even good faith belief in an immediate emergency threat to life or limb. Instead, the emergency exception is reserved for specific emergency situations "in which time is of the essence and requiring that a court order be obtained would cause delay which could result in severe jeopardy for a victim of crime." *In re Application of U.S. for Nunc Pro Tunc Order for Disclosure of Telecommunications Records*, 352 F. Supp. 2d 45, 47 (D. Mass. 2005) (declining to issue retroactive court order authorizing telecommunications provider's voluntary disclosure of records concerning a kidnapping for ransom because the statute does not provide for such orders, opining in *dicta* that such an order was unnecessary to shield the provider from potential liability because its conduct fit the emergency exception).

Case law interpreting the emergency exception for interceptions under Title III, which uses language substantially identical to that in the emergency exception for records,[9] further supports the conclusion that such exceptions are reserved for specific and urgent threats to life or limb, and cannot justify conduct extending beyond a few hours or days—much less the several years alleged here. *See, e.g., U.S. v. Capra*, 501 F.2d 267, 277, 277 n.8 (2d Cir. 1974) (refusing to apply emergency exception to eavesdropping that continued for 17 days, noting that "Congress had in mind by use of the term 'emergency' an important event, limited in duration, which was likely to occur before a warrant could be obtained"). This is because emergencies are by definition urgent and unexpected events that are themselves likely to occur within a matter of hours or days. *See, e.g., U.S. v. Crouch*, 666 F. Supp. 1414, 1416-17 (N.D. Cal. 1987) (citing *Capra* and holding that reliable information that suspects with violent records were planning a bank robbery sometime in the next 60 days did not suffice to establish an emergency). In sum, no

[9] 18 U.S.C. § 2518(7) authorizes the government to conduct interceptions without a warrant when it "reasonably determines that . . . an emergency situation exists that involves . . . immediate danger of death or serious injury to any person," so long as it seeks court approval within 48 hours. *Id.*

fair reading of the emergency exception created by the PATRIOT Act could excuse Verizon's disclosure of millions of customers' records over a period of years, *see* MCC ¶ 166, especially where Verizon has offered no evidence demonstrating its good faith belief in an immediate emergency.[10]

C. The "Rights or Property" Exception Cannot Be Fairly Read to Authorize the Alleged Disclosures.

Verizon also fails in its claim that the exception at 18 U.S.C. § 2702(c)(3), allowing the disclosure of records "as may be necessarily incident to . . . the protection of [its] rights or property," can be fairly read to justify dismissal, Ver. Mem. at 44-45. A brief look at the history of this exception and the Title III exception from which its language is taken[11] demonstrates that it does not apply to Verizon's disclosures, as alleged in the Master Complaint.

The "rights or property" exception originated prior to Title III's enactment, as a common law defense against claims based on 47 U.S.C. § 605's prohibition on the interception and disclosure of communications by communications carriers. *See United States v. Beckley*, 259 F. Supp. 567, 571-572 (N.D. Ga. 1965) (*quoting Casey v. United States*, 191 F.2d 1, 4 (9th Cir. 1951), *reversed on other grounds*, 343 U.S. 808 (1952)). This common law defense, particularly as construed by the Ninth Circuit, was and is limited to reasonable measures taken by communications carriers to combat fraudulent (*i.e.,* unpaid) use of their services. *See, e.g., Bubis v. United States*, 384 F.2d 643, 647-48, 648 n.5 (9th Cir. 1967). As the Court stated:

---

[10] Nor can the 2006 amendments to the statute excuse Verizon's actions. Although the word "immediate" has been removed, the exception still requires a life-threatening "emergency" situation requiring action "without delay," 18 U.S.C. § 2702(c)(4), and such language cannot be fairly read to comprehend an extended, generalized, years-long state of perpetual emergency. The exception also still requires proof of Verizon's belief in such an emergency—a "good faith" rather than a "reasonabl[e]" belief. *Id.* Perhaps most importantly, the latest codification clarifies that a provider may only disclose information "relating to the emergency." 18 U.S.C. § 2702(c)(4). Therefore, the exception plainly cannot apply, since Verizon's wholesale disclosures necessarily included records concerning millions of innocent Americans with no possible connection whatsoever to any terrorist organization, members, or plot.

[11] 18 U.S.C. § 2511(2)(a)(i) provides that "It shall not be unlawful . . . for . . . a provider of wire or electronic communication service . . . to intercept, disclose, or use [a] communication . . . while engaged in any activity which is a *necessary incident . . . to the protection of the rights or property* of the provider of that service . . . ." *Id.* (emphasis added).

> When a subscriber of a telephone system uses the system's facilities in a manner which *reasonably justifies* the telephone company's belief that he is violating his subscription rights, then he must be deemed to have consented to the company's monitoring of his calls to *an extent reasonably necessary* for the company's investigation.

Id. at 648 (emphasis added), *citing Brandon v. United States*, 382 F.2d 607 (10th Cir. 1967) and cases therein cited.

In enacting Title III, Congress intended that statute's "rights or property" exception to preserve and codify this common law exception. *See* 1968 U.S.C.C.A.N. 2112, 2182 (noting Congress's intent that the "rights or property" exception reflect existing law and citing *Beckley*). Accordingly, the federal courts—and, again, the 9th Circuit in particular—have continued to narrowly construe the Title III exception so as to reach only reasonable conduct targeted at fraudulent use of a communications provider's services. *See Goldstein*, 532 F.2d at 1311; *accord Hodge v. Mountain States Telephone and Telegraph Company*, 555 F.2d 254, 260 n.16 (9th Cir. 1977). Furthermore, Title III's "rights or property" exception ceases to apply as soon as the provider acts at the request of the government:

> [The government is] not free to ask or direct [the phone company] to intercept any phone calls or disclose their contents, at least not without complying with the judicial authorization provisions of [Title III], regardless of whether [the company] would have been entitled to intercept those calls on its own initiative.

McClelland v. McGrath, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (discussing exception). Put simply, Title III's "rights or property" exception is exceedingly limited, allowing only reasonable conduct undertaken as necessary to combat fraudulent use of a provider's services, and cannot be used as a loophole to justify surveillance undertaken at the government's direction.

Just as Title III's exception is limited, so is the "rights or property" exception for the disclosure of records. The PATRIOT Act's legislative history and the plain language of 18 U.S.C. § 2702(c)(3) confirm that Congress intended the "rights or property" exception for records disclosures to mirror the limited exception in Title III. *See id.* (using language identical to that in Title III exception); 147 Cong. Rec. S. 10365, 10371 (describing "rights or property" exception as authority "to protect against fraud"). As such, it simply cannot be read to justify Verizon's manifestly unreasonable, massive, and years-long disclosure of millions of records to the government.

III. THERE IS NO IMPLICIT EXCEPTION FOR CONDUCT RELATED TO FOREIGN INTELLIGENCE GATHERING JUSTIFYING DISMISSAL OF THOSE CLAIMS.

Title III and ECPA both apply to Verizon's interception and disclosure of Plaintiffs' communications and records, as shown by the plain language of the statutes. Verizon attempts to argue that conduct related to foreign intelligence gathering is implicitly excepted from those statutes' reach. However, Congress specifically addressed these issues when it enacted 18 U.S.C. § 2511(2)(f), which provides:

> Nothing contained in this chapter or chapter 121 or 206 of this title [18 U.S.C. §§ 2510 *et seq*., or 2701 *et seq*., or 3121 *et seq*.], or section 705 of the Communications Act of 1934 [47 U.S.C. § 605], shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means *other than electronic surveillance* as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801], and *procedures in this chapter or chapter 121 or 206 of this title* [18 U.S.C. §§ 2510 *et seq*., 2701 *et seq*., or 3121 *et seq*.] *and the Foreign Intelligence Surveillance Act of 1978* [50 U.S.C. §§ 1801 *et seq*.] *shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act* [50 U.S.C. § 1801], *and the interception of domestic wire, oral, and electronic communications may be conducted*.

(Emphasis added.) As discussed below, this exception does not apply to the conduct alleged here.

A. There is No Implicit Exception to Title III

Verizon argues that Title III does not apply to surveillance conducted for foreign intelligence purposes. This argument is without merit.

First, the plain language of Title III covers the conduct alleged here. *See* 18 U.S.C. § 2511(1) ("Except as otherwise specifically provided in this chapter [18 U.S.C. § 2510 *et seq*.] any person who intentionally intercepts any wire, oral, or electronic communication shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).").

Verizon asks this Court to disregard the statutory text in favor of a tortured construction of FISA and Title III that no court has ever accepted.[12]

Second, the language and structure of Title III, and the legislative history of FISA, clearly demonstrate that the same conduct can violate both statutes. Title III generally prohibits interception, *i.e.*, the acquisition by device of the contents of oral, wire and electronic communications, by anyone, 18 U.S.C. § 2511(1), and then creates exceptions to that general prohibition. *See generally* 18 U.S.C. § 2511(2). Obtaining a valid judicial interception order is one of those exceptions. 18 U.S.C. §§ 2516, 2518.

Prior to FISA's enactment, Title III refrained from regulating foreign intelligence surveillance. 18 U.S.C. § 2511(3) ("[N]othing . . . shall limit the constitutional power of the President . . . to obtain foreign intelligence information."), Act of June 19, 1968, Pub. L. No. 90-351, § 2511, 82 Stat. 197, 214. This provision indicates that, by its terms, Title III *would* have regulated foreign intelligence surveillance, absent this express reservation.

After the Church Committee's demonstration of the Executive Branch's massive abuses of "national security" surveillance,[13] however, Congress adopted FISA "to curb the practice by which the executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 8, 1978 U.S.C.C.A.N. 3904, 3910. In so doing, Congress repealed 18 U.S.C. § 2511(3). *See* FISA, Pub. L. No. 95-511, § 201(c).

---

[12] Verizon quotes *U.S. v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992), and *U.S. v. Torres*, 751 F.2d 875 (7th Cir. 1985), out of context; neither case applies here. The defendants in both cases argued that FISA, which subjects silent video surveillance to its judicial authorization procedures, should also protect them. Silent video surveillance, however, cannot violate Title III, because it is "impossible for silent television surveillance to intercept a 'wire, oral, or electronic communication.'" *Koyomejian*, 970 F.2d 536 at 541 (9th Cir. 1992) (internal quotation marks and citation omitted). The courts in *Koyomejian* and *Torres* analyzed the relationship between FISA and Title III only in order to address the argument that FISA authorization was required even though Title III did not prohibit silent video surveillance. Here, by contrast, plaintiffs have clearly alleged interception, which can violate both FISA and Title III.

[13] The United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known informally as the "Church Committee" after its Chairman, Sen. Frank Church, concluded "that warrantless electronic surveillance in the name of national security ha[d] been seriously abused." S. Rep. No. 95-604(I) at 7-8 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3908-09; *see S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong., S. Rep. No. 94-755 (1976) (Church Committee Books I-VI), available at http://www.aarclibrary.org/publib/church/reports/contents.htm; *see also United States v. Belfield*, 692 F.2d 141, 145-46 (D.C. Cir. 1982) (discussing FISA's history). The Committee concluded that "[t]he Constitutional system of checks and balances ha[d] not adequately controlled intelligence activities" (Church Committee Book II at 6), and recommended that the NSA be limited by "a precisely drawn legislative charter" (*id*. at 309).

As the text of FISA shows, Congress did not establish a parallel, freestanding regime of foreign intelligence surveillance. Rather, Section 201(b) of FISA amended Title III to create an integrated regime that regulates *all* executive branch surveillance. *See* 18 U.S.C. § 2511(2)(f). Furthermore, to the extent that § 2511(2)(f) refrains from regulating some foreign intelligence collection, those areas are expressly restricted to means "*other* than electronic surveillance." *Id.* (emphasis added). Thus, Title III (and 47 U.S.C. § 605[14]) can and do apply to "electronic surveillance", because § 2511(2)(f) only exempts activities that are *not* "electronic surveillance."

In short, FISA extended Title III to regulate all interceptions, even those conducted for foreign intelligence purposes, which is why Congress made clear that electronic surveillance that complies with FISA's procedures is excepted from Title III's general prohibition on interception:

> Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

18 U.S.C. § 2511(2)(e).

---

[14] In passing, Verizon also argues that 47 U.S.C. § 605 does not apply to interception of communication contents for the purpose of gathering foreign intelligence. Verizon Mem. at 14 (*quoting United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974) (*en banc*)). But pre-FISA cases like *Butenko* mean nothing here, given that § 2511(2)(f) expressly refers to 47 U.S.C. § 605; contrary to *Butenko* and Verizon's argument, Congress clearly did consider whether § 605 reaches foreign-intelligence gathering, and chose not to make any exception for domestic communications or domestic electronic communications systems.

Verizon also categorically asserts that 47 U.S.C. § 605 does not apply to disclosure of call *records* by citing one inapposite case, *United States v. Barnard*, 490 F.2d 907 (9th Cir. 1973). Ver. Mem. at 46. The only Section 605 issue in *Barnard* was whether in a criminal trial on a motion to suppress "Section 605 . . . rendered *evidentially inadmissible* the records made in the ordinary course of a telephone company's business." *Id.* at 913 (emphasis added). In the more relevant context of a civil trial against telephone companies for invasion of privacy based on unauthorized interception of call records, multiple federal circuit courts have found 47 U.S.C. § 605 applicable. *See Brown v. Continental Telephone Company of Virginia*, 670 F.2d 1364, 1365-66 (4th Cir. 1982) (applying Section 605 to privacy suit for disclosure of telephone records, and finding Section 605 authorized release of records pursuant to subpoena issued by court).

Finally, and further belying Verizon's argument that Title III is a completely separate statutory regime, FISA § 201(a) amended Title III to provide that no person may assist in government surveillance without either a court order requiring such assistance or a certification that the surveillance is legal, under *either* Title III or FISA:

> Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—
>
> (A) a court order directing such assistance signed by the authorizing judge, or
>
> (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

18 U.S.C. § 2511(2)(a)(ii). This section predates FISA, but FISA substantially revised it—and the House Intelligence Committee explicitly articulated its intent to "extend [the] scope" of the § 2511(2)(a)(ii) court order or certification requirement "to cover foreign intelligence electronic surveillance." H.R. Rep. No. 95-1283, at 98 (1978). *See* 50 U.S.C. § 1801(e) (2006) (defining "foreign intelligence," unchanged from the 1978 version).

Thus, Title III provides that a person with a valid court order or certification under either Title III or FISA may assist the government. Conversely, if a person assists the government in conducting surveillance without a court order or certification, he is explicitly liable for damages under 18 U.S.C. § 2520, and under 50 U.S.C. § 1810 as well.

B. There is No Implicit Exception to ECPA

Verizon asserts that as a matter of law, it cannot violate ECPA by disclosing customer records to the government for foreign intelligence purposes, because ECPA only restricts disclosure to law enforcement officials. The plain language of the statute refutes this argument:

> a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to *any governmental entity*.

18 U.S.C. § 2702(a)(3) (emphasis added).

ECPA broadly prohibits disclosure of customer records to the government, while exempting some disclosures for specific purposes. *See, e.g.*, 18 U.S.C. §§ 2702(c)(3) (voluntary disclosures for protection of service provider's rights or property); 2702(c)(4) (voluntary disclosures in emergencies involving immediate danger of death or serious physical injury to any person); § 2703(e) (no cause of action against service providers that disclose information, facilities or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter). Congress knew how to—but did not—write an exception for voluntary disclosure to the government for foreign intelligence purposes. Therefore, Verizon violated ECPA by voluntarily disclosing customer records to the government.

Verizon asserts that the plain language of the records provisions confirms that it deals only with law enforcement. Ver. Mem. at 12. But § 2702(a)(3) broadly prohibits disclosure of customer records to "any governmental entity," not to "any law enforcement agency." Indeed, Congress expressly used the phrase "law enforcement agency" in one exemption, 18 U.S.C. § 2702(b)(7). This provision demonstrates that Congress intentionally distinguished governmental entities from law enforcement agencies in the statute.

Moreover, while Congress did not generally exempt disclosures for foreign intelligence purposes, it addressed this issue in a separate provision providing that with appropriate process, the FBI may obtain subscriber information, toll billing information, and electronic communication transactional records that are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709. Indeed, § 2709 as originally enacted expressly required "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801)." Public Law 99-508, Sec. 201 (1986); *id.*, Sec. 107(a) ("Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity").[15] The plain language of the statute unquestionably reaches more than law enforcement.

Finally, Verizon argues that because 18 U.S.C. § 2511(2)(f) only applies to communication contents, Congress did not mean to impair the executive's ability to collect communication records for foreign intelligence purposes. But even if § 2511(2)(f) could be read as Verizon suggests, it would not permit the executive to collect foreign intelligence information ("FII") from *domestic* communications or domestic electronic communications systems, as Plaintiffs have alleged, as it is limited to "international or foreign communications" or "foreign intelligence activities . . . involving a foreign electronic communications system." 18 U.S.C. § 2511(2)(f)[16]; *see* 18 U.S.C. § 2510(19) (defining "foreign intelligence information"). Congress clearly chose *not* to exempt the acquisition of information from *domestic* communications from ECPA. Nor, as a factual matter, could all of the customer records that Verizon disclosed possibly contain FII.

Verizon asks this Court to create a new exception for foreign intelligence matters even though Congress has already created one. The plain language of the statute is clear, and therefore the Court need not look to the legislative history of the Act. *See, e.g.*, *W. Va. Univ. Hosps. v. Casey*, 499 U.S. 83, 98-99 (1991) (citing *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989) ("Where, as here, the statute's language is plain, the sole function of the courts is to enforce it according to its terms.") (internal citations omitted)).

IV. THE AUMF DID NOT CREATE SUCH AN EXCEPTION

Verizon next argues that Congress authorized the President to violate ECPA when it passed the AUMF. *See* Ver. Mem. at 20. This argument, which is *not* advanced by the government, misinterprets the AUMF. The AUMF authorizes the President to use "all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons."[17] The AUMF does not mention, or even imply, the authorization of electronic surveillance or domestic intelligence gathering.[18]

---

[15] These two provisions, along with 18 U.S.C. § 2511(2)(f), refute Verizon's argument that Congress did not make a "clear statement" of intent to limit Presidential power in ECPA. Ver. Mem. at 18-19. Furthermore, Verizon's argument that the President would be unable to collect many types of records if ECPA were so construed, Ver. Mem. at 18, fails because FISA court orders can be used "to obtain foreign intelligence information… to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § 1861.

[16] That Congress expressly included ECPA ("chapter 121 . . . of this title") in § 2511(2)(f) further undermines Verizon's argument that ECPA is silent as to Presidential national security authority.

Post-AUMF Congressional amendments to FISA, none of which eliminated its strong warrant provisions, also demonstrate that Congress never intended the AUMF to authorize electronic surveillance outside the framework of FISA.[19] Moreover, even if the AUMF could plausibly be read to authorize intelligence activities, Title III, FISA, and ECPA are highly specific statutes governing the interception and disclosure of communications and communications records. They must prevail over the more general AUMF. *See Edmond v. U.S.*, 520 U.S. 651, 657 (1997); *see also Morales v. TWA, Inc.*, 504 U.S. 374 (1992) ("it is a commonplace of statutory construction that the specific governs the general"). The AUMF does not, and cannot be applied to undermine the specific statutory scheme governing the conduct at issue here.

In *Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006), the Supreme Court rejected the argument that the AUMF implicitly authorized the President to create a system of military commissions at Guantanamo Bay, Cuba that differed in significant respects from those authorized from the commissions authorized by Article 21 of the Uniform Code of Military Justice. As the Court stated, "there is nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth in Article 21 of the UCMJ." *Hamdan*, 126 S. Ct. at 2775 (footnote omitted). The same reasoning applies here. While the AUMF may authorize activities that are "accepted incident[s] of war," the interception and disclosure of Plaintiffs' communications and records do not fall within the purview of such authorization.

---

[17] Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541).

[18] *Cf. Wartime Executive Power and the NSA's Surveillance Authority (Part I): Hearing Before the Senate Judiciary Committee*, 109th Cong., at 186 (2006) (Senator Lindsey Graham (R-SC)) ("I will be the first to say when I voted for it, I never envisioned that I was giving to this President or any other President the ability to go around FISA carte blanche."); *id.* (Senator Arlen Specter (R-PA)) ("I do not think that any fair, realistic reading of the September 14 resolution gives [the President] the power to conduct electronic surveillance"); *see also ACLU v. Nat'l Sec. Agency/Central Sec. Serv.*, 438 F. Supp. 2d 754, 779 (D. Mich. 2006) ("[T]his court must note that the AUMF says nothing whatsoever of intelligence or surveillance.").

[19] Congress first deleted a former requirement for certification that the primary purpose of a surveillance is to gather foreign intelligence information. 115 Stat. 272, §§ 206-108, 214-218, 504, 1003. Congress then amended FISA by increasing the emergency warrantless surveillance period from 24 hours to 72 hours. 115 Stat. 1394, § 314(a)(2)(B) (Dec. 28, 2001).

Hamdi v. Rumsfeld, 542 U.S. 507 (2004), provides no support for Verizon's argument that warrantless surveillance falls under the AUMF's authorization for "all necessary and appropriate force" against al Qaeda. Unlike in *Hamdi*, millions of Americans living in the United States who make or receive phone calls are not members of al Qaeda or enemy combatants engaged with the enemy on the battlefield. They are outside the scope of the AUMF. In fact, when the Administration sought to include the words "in the United States" after the words "appropriate force" to authorize domestic as well as foreign actions, Congress flatly rejected the request. *See* Tom Daschle, *Power We Didn't Grant*, WASH. POST, Dec. 23, 2005, at A21.

Congress's rejection of the request was in accordance with "[o]ur history and tradition," which "rebel at the thought that the grant of military power carries with it authority over civilian affairs." *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579, 632 (1952) (Jackson, J., concurring). The President's war powers, even broadly construed, cannot provide a justification for unchecked intrusion into the communications of Americans and others residing within this country.[20]

---

[20] *Cf. Youngstown*, 343 U.S. at 642 ("[N]o doctrine that the Court could promulgate would seem to me more sinister and alarming than that a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture."); *id.* at 587 (majority opinion) ("Even though the 'theater of war' be an expanding concept . . . This is a job for the Nation's lawmakers, not for its military authorities"); *Hamdi*, 542 U.S. at 537 ("Any process in which the Executive's factual assertions go wholly unchallenged or are simply presumed correct without any opportunity for the alleged combatant to demonstrate otherwise falls constitutionally short.").

V. CLAIMS AGAINST VERIZON FOR INTERCEPTION AND DISCLOSURE DO NOT REQUIRE ALLEGATIONS OF HUMAN REVIEW BY NSA ANALYSTS.

Verizon next attempts to misconstrue the allegations of the complaint, repeatedly referring to Plaintiffs' allegations of the "inclusion" of information in a database, Ver. Mem. at 23, 38, and the "extract[ion]" of information from a database, *id.* at 22-23, 25. It's not clear exactly what Verizon is arguing, as those words do not appear in the Master Complaint. However, Verizon *seems* to be making two arguments, both baseless: First, that Plaintiffs have failed to state a claim if they only alleged that Verizon allowed the NSA "access" to its networks and databases to scan Plaintiffs' communications and records with computer programs and "extract" foreign intelligence information, as opposed to directly handing over or transmitting Plaintiffs' communications and records to the government; and second, that even if Plaintiffs' *did* allege such a hand-over to the government, the claims fail because Plaintiffs did not allege that government agents personally reviewed the communications and records. We will address this second and most outrageous argument first.

A. Claims of Interception Do Not Require Allegations of Human Review.

Without any support, and in contradiction to the statutes' plain language, Verizon unfairly reads Title III and FISA's plain prohibitions on the "acquisition" of communications content by a "device"[21] to only prohibit the "examination" of those contents by a "human." Ver. Mem. at 9. Federal courts have considered and consistently rejected this argument. *See, e.g., U.S. v. Rodriguez,* 968 F.2d 130, 136 (2d Cir. 1992) (holding that "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time.").[22] This argument also defies common sense: it would be impossible for the NSA to scan (or "sift")

[21] *See* 18 U.S.C. § 2511 and 50 U.S.C § 1801(f) (definitions of "intercept" and "electronic surveillance," respectively).

[22] *See also In re State Police Litigation*, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (holding that "it is the act of diverting, and not the act of listening, that constitutes an 'interception.'"); *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (same); *U.S. v. Lewis*, 406 F.3d 11, 18 n.5 (1st Cir. 2005) (same); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994) (same); *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994) (same); *see also Awbrey v. Great Atlantic & Pacific Tea Co.*, 505 F. Supp. 604, 606-607 (N.D. Ga. 1980) (allegations of continued, indiscriminate wiretapping sufficient to survive motion for summary judgment without evidence of specific phone calls tapped).

Plaintiffs' communications with computer devices[23] unless they have first been *acquired* by a device. Indeed, Verizon's argument that an interception is not an interception absent human review actually contradicts the cases it cites in support.

First, the initial *Halkin v. Helms* decision does not support Verizon's argument, as is made clear when reading the sentence immediately following the one that Verizon quotes: "NSA computers scan the mass of *acquired communications* to select those which may be of foreign intelligence interest." *Halkin v. Helms*, 598 F.2d 1, 4 (D.C. Cir. 1978) (*Halkin I*) (emphasis added). In other words, the NSA does not (and practically, cannot) scan a communication until the communication's "signals" are first "acquired by [the NSA's] many techniques." *Id.* *Halkin* certainly did not hold that "to establish that their calls were 'acquired,' plaintiffs would need to prove that their calls were selected by the computers for human examination." Ver. Mem. at 10. Rather, *Halkin I* only held that the "mere existence" of plaintiffs' names on the NSA's watchlists or intelligence reports could not support the presumption that their communications were among the mass of communications that were actually *acquired*. *Id.* at 10-11.

Second, *Sanders v. Robert Bosch Corp*. is of no help to Verizon, as its pertinent holdings were (1) that "there [was] no evidence that any Bosch employee ever listened to, recorded, or *otherwise acquired* any conversations from the [guards'] office by means of the open microphone," as opposed to acquiring only content-less "ambient noise," and (2) that the defendants did not mean to leave the microphone on and therefore did not *intentionally* intercept any conversations that were acquired by the open microphone. 38 F.3d 736, 742-43 (4th Cir. 1994). Indeed, *Sanders* contradicts Verizon's argument, holding that a finding of "interception" does *not* turn on whether a person listened to the intercepted communications, only on whether they were acquired by a device in the first place. *Id.* at 740.

Finally, Verizon's citation to a case considering the meaning of unauthorized "access" to a communications facility in violation of 18 U.S.C. § 2701 is wholly inapt. Ver. Mem. 10, *citing*

---

[23] Verizon repeatedly cites to such allegations, Ver. Mem. 9-10, 23, 25, even though they are ultimately unnecessary to maintaining Plaintiffs' claims, *see Hepting*, 439 F. Supp. 2d at 994, 999.

United States v. Smith, 155 F.3d 1051 (9th Cir. 1998). Plaintiffs have plainly alleged that Verizon "*actually* acquire[d]" for the government "the contents of [Plaintiffs'] communications" with surveillance devices, *Smith*, 155 F.3d at 1058 (emphasis in original), and/or assisted the government in acquiring the same. MCC ¶¶ 163, 168, 173-75, 230, 245. Plaintiffs have not alleged unauthorized access under § 2701—indeed, they allege that Verizon authorized and assisted in the NSA's use of its facilities, MCC ¶ 173—and the fact that the Master Complaint (or news reports cited therein) occasionally describes Verizon's conduct as providing "access" is of no moment under notice pleading standards.

In sum, claims of interception do not require the allegation that humans actually reviewed the acquired communications. Nor do claims for disclosure of communications or records require that the party to whom they were disclosed chose to examine them personally, as discussed next.

B. Claims Against Verizon for Disclosure of Plaintiffs' Communications and Records Do Not Require Allegations of Human Review by NSA Analysts, and Allegations that Verizon "Divulged," "Disclosed," "Provided" and/or "Provided Access To" Plaintiffs' Communications and Records Are More Than Sufficient.

Verizon puts forward an unprecedented argument: that Plaintiffs' claims against Verizon's "divulgence" of Plaintiffs' communications and records under 18 U.S.C. § 2702(a) require an allegation that a Verizon employee has actually shown or read those communications and records to an NSA analyst, *i.e.*, has made that information personally "known" via the eyes and ears of a human being at the NSA. Ver. Mem. at 24 (citing dictionary definition of "divulge"). Verizon apparently argues that even an allegation that it mailed copies of Plaintiffs' communications and records to the NSA would not suffice, unless accompanied by the allegation that an NSA agent actually picked the package up from the mailbox, opened it, and then personally reviewed the entirety of the package's contents. *Id*. Such a strained and improbable reading of 18 U.S.C. § 2702 not only renders it virtually unenforceable, but is flatly inconsistent with the statute's plain language and structure, as well as common law and constitutional principles.

First, regardless of Verizon's reading of the word "divulgence," Plaintiffs plainly pleaded that Verizon did "divulge" their communications and records.[24] These plain allegations are more than sufficient to survive a motion to dismiss. That Plaintiffs or the press reports they cite refer to this act of "divulging" as "disclosing," "providing," or "providing access to" communications and records is irrelevant; both the dictionary and Congress treat these terms synonymously, and neither indicates the need to establish "scrutiny by human eyes." Ver. Mem. at 23. For example, Congress plainly considers "divulgence" to be a synonym of "disclosure" based on its repeated use of that term to describe the act regulated by 18 U.S.C. § 2702, a section tellingly entitled "voluntary *disclosure* of customer communications or records." *See id*. (emphasis added); *see also id.* at (b)-(c) (listing "exceptions for *disclosure*" of communications and customer records (emphasis added)). Notably, the verb "disclose," while sharing the definition "to make known" with "divulge," also is defined as "to expose to view, as by removing a cover," or to "reveal," *The American Heritage® Dictionary of the English Language, Fourth Edition,* Houghton Mifflin Company, 2004, which would encompass both "providing" information (making it "available" or "furnish[ing]" it, *id.*) as well as providing "access" to information ("access" being "the ability or right to approach, enter, exit, communicate with, or make use of," *id.*). Plaintiffs have pleaded all of these acts.

Verizon complains of Plaintiffs' use of the term "provide," arguing that "[i]f Congress intended to prohibit providing access to a database, it would have chosen a broader word than 'divulge,' such as to '*provide*'…." Ver. Mem. at ¶ 25 (emphasis in original). But Congress clearly stated its intent that the act of "divulging" be synonymous with that of "providing" (as well as "disclosing"). *See* H.R. Rep. No. 99-647, at 64 (1986) (describing the term "divulgence" in Title III and ECPA's prohibitions as including "the act of *disclosure*[;] [t]he result is that the [information] ha[s] been *provided* to another person or entity" (emphasis added)). The verb "provide," moreover, does not require that the recipient personally "know" that information through human perception – only that it be "ma[de] available" or "furnished" to the recipient. *The American Heritage® Dictionary of the English Language, Fourth Edition*.

---

[24] Verizon's claim that "[P]laintiffs allege *only* that defendants provided NSA access to databases that NSA could search, … not that any information about them was actually "divulged" to any person in the government[,]" Ver. Mem. at 25 (emphasis added), is demonstrably false, *see, e.g.,* MCC ¶¶ 158 ("A June 30, 2006 USA Today story reported that 19 members of the intelligence oversight committees of the U.S. Senate and House of Representatives 'who had been briefed on the program verified that *the NSA has built a database that includes records of Americans' domestic phone calls*,' and that four of the committee members confirmed that 'MCI, the long-distance carrier that Verizon acquired in January, did *provide call records to the government*.'") (emphasis added)); 163 ("Defendants MCI and Verizon knowingly and intentionally *provided and continue to provide the aforementioned telephone call contents and records to the federal government*."); 169 ("MCI and Verizon have *disclosed and/or divulged the "call-detail records" of all or substantially all of their customers, including Plaintiffs, to the NSA*") (emphasis added). Of course, as discussed later in this section, even an allegation of providing "access" alone would be sufficient.

Verizon's desperate resort to dictionary definitions to attack Plaintiffs' well-pleaded claims also ignores the statute's structure. ECPA's prohibitions on "divulgence" regulate what *providers* like Verizon may lawfully *do*, not what *government agents* may lawfully *perceive*; thus, allegations about the government's conduct are unnecessary. *See Hepting*, 439 F.Supp.2d at 994, 999. Liability for such "divulgences" cannot turn on what the government *did* with a plaintiff's communications and records after they were handed over by a communications provider. Indeed, Verizon fails to cite, and Plaintiffs have failed to find, *any* case where a court has held (or even considered the argument) that a communications provider has not "divulged" information to the government until government agents read or listen to the information delivered into their possession.

As a last resort, Verizon argues that this Court should look to *defamation law* to resolve the purported "ambiguity" in the statute. This is wholly unnecessary considering the statute's plain meaning and the Master Complaint's well-pleaded allegations. However, should this Court choose to look to the common law, the obvious and proper analogue is *invasion of privacy*, not defamation. The tort of intrusion upon seclusion does *not* require that a plaintiff establish that the defendant actually examined or published any private information, only that the defendant "obtained unwanted *access* to data about the plaintiff." *Shulman v. Group W Productions*, 18 Cal. 4th 200, 232 (1998) (holding that "the mere placement of the surveillance equipment on the shelf in plaintiffs' office itself invaded their privacy because it allowed the defendants…to 'activate' the surveillance system at any time during the day without plaintiffs' knowledge, thus at least presenting the possibility of unwanted *access* to private data about plaintiffs") (emphasis added); *see also* Rest.2d Torts, § 652B, comment b ("The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined").

Finally, this Court must consider the *constitutional* values Congress sought to enforce through Title III and ECPA. In the landmark case of *Berger v. New York*, 388 U.S. 41 (1967),[25] the Supreme Court's primary concern was that the eavesdropping statute at hand gave the government unchecked discretion to invade privacy, a "roving commission to 'seize' any and all conversations." *Id*. at 51. This concern echoes the Founders' concerns about general warrants, "the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980). Just as Congress intended to limit the government's discretion in Title III, it sought in ECPA to statutorily ensure that the Fourth Amendment's constraints on the government's discretion not be outpaced by changing technology. S. REP. NO. 99-541, at 5, 1986 U.S.C.C.A.N. 3555 (1986) (stating that "[m]ost importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment").

Verizon's argument would leave its liability and Plaintiffs' privacy solely to the discretion of NSA's analysts, much as a general warrant would allow "a general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). Looking to Fourth Amendment values in construing Title III and ECPA's constraints on Verizon, however, it is clear that "nothing [should be] left to the discretion of the [government's] officer[s]." *Id.* Any other holding would leave the privacy of all Americans' communications and records at the mercy of individual government agents.

VI. PLAINTIFFS' CLAIMS FOR VIOLATIONS OF ECPA DO NOT RUN AFOUL OF THE FIRST AMENDMENT.

Verizon is off base in its claim that the First Amendment's Speech and Petition Clauses immunize its intentional wholesale violation of a Congressional statute designed to protect Americans' privacy. Verizon's argument, if accepted, would undermine a wide swath of laws

[25] Congress intended to implement *Berger*'s restrictions on surveillance in Title III. *Bartnicki v. Vopper*, 532 U.S. 514, 522-23 (2001).

that protect privacy and confidentiality. As demonstrated below, however, Verizon's arguments are fatally flawed.

First, strict scrutiny is inapplicable for two different reasons: (1) the government's purpose in prohibiting disclosure of customer records by telecommunications companies is content neutral; and (2) Verizon's ongoing transfer of its customers' records to the government is not speech on a matter of public concern, rendering inapposite the media publication cases on which Verizon chiefly relies. Second, applying the proper standard—either the less formulaic balancing used by the Supreme Court in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), or intermediate scrutiny—the privacy and private-speech facilitating interests protected by ECPA outweigh any interest Verizon has in giving its customers' records to the NSA. Third, the Petition Clause provides no more or different protection than the Speech Clause, and any interest that Verizon has in petitioning the government does not require the company to engage in the wholesale disclosure of its customers' records. Finally, the *Noerr-Pennington* doctrine does not immunize Verizon from a knowing violation of settled law.

A. If Accepted, Verizon's Argument Would Eviscerate a Broad Swath of Non-Disclosure Laws and Statutory Duties of Confidentiality.

While Verizon's First Amendment argument is directed to ECPA, it is important to consider the likely scope and implication of its argument. At bottom, if Verizon's argument were correct, then the whole fabric of federal non-disclosure laws would likely be unconstitutional under the First Amendment. Its analysis would immunize the wholesale disclosure of the most sensitive private information, even though expressly prohibited by statute.

The Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3401 *et seq.*, provides a good example. That Act prohibits banks and credit card issuers, among others, *id.* at 3401(1), from disclosing financial records to the government except under specific circumstances, such as where the customer authorizes the disclosure, or the government obtains a warrant. 12 U.S.C. § 3402. Under Verizon's interpretation of the First Amendment, the statute would be unconstitutional.

First, Verizon would argue that the Act is a content-based restriction on disclosure: it applies only to financial records. Second, financial institutions lawfully obtain the records of their customers—creation of records detailing sensitive financial information provided by customers is an inevitable consequence of transacting business with these entities. Third, like Verizon, a bank could argue that the wholesale disclosure of its customer records to the NSA is "speech" on a matter of public concern—providing these records would aid in the fight against terrorism by allowing the government to search for patterns of transactions that might reveal the existence of a terrorist financial network. Hence, as Verizon would have it, before a financial institution could be sanctioned for providing copies of all of its customers' records to the NSA, application of RFPA must survive strict scrutiny. Just as Verizon does here, a bank would argue that Congress' interest in protecting privacy is not a compelling one, and that therefore the statute is unconstitutional.

RFPA is but one of a number of important federal privacy statutes that would be vulnerable if Verizon's understanding of the First Amendment were correct, including:

- The Health Insurance Portability and Accountability Act (HIPAA), imposing fines and criminal punishments for the knowing disclosure of "individually identifiable health information to another person." 42 U.S.C. § 1320d-6.
- The Fair Credit Reporting Act, 15 U.S.C. § 1681, prohibiting consumer reporting agencies from disclosing credit reports except in delineated circumstances.
- The Family Education and Privacy Rights Act (FERPA), 20 U.S.C. § 1232g(b), prohibiting educational institutions receiving federal funds from disclosing "education records" except in specified circumstances.

The scope of Verizon's argument does more than threaten current federal privacy law, however. Any number of privileges, most of which are codified by statute and all of which are designed to facilitate communication among private parties by ensuring privacy, would be vulnerable. The attorney's duty of confidentiality, and the psychotherapist-patient confidentiality obligation, applying to only certain categories of communications between the parties, are two obvious examples. Thus, law firms such as Wilmer Cutler Pickering or Munger Tolles & Olson could claim the right to provide the government with records for all their clients in South America or the Middle East, arguing that by helping the government fight the war on drugs or the war on terror, they, too, are disclosing information on a matter of public concern.[26]

Each of the foregoing federal and state statutes and privileges would be vulnerable to attack under Verizon's thesis here. Verizon would contend that each is a content-based prohibition on disclosure. Because a decision by each of the regulated entities to engage in wholesale disclosure of these otherwise lawfully obtained private records could be rationalized in some generalized fashion as necessary to aid the government in addressing national security or some other public safety concern, Verizon would characterize each such mass disclosure as speech on a matter of public concern. Thus, although each prohibition on disclosure facilitates private speech among private parties by ensuring the privacy of their communications, Verizon would have this Court conclude that strict scrutiny applies to invalidate each of these statutes under the First Amendment. As discussed below, that is not the law.[27]

B. **ECPA's Customer Record Provisions Are Content Neutral, Because They Further the Content Neutral Purpose of Promoting Customer Privacy and Private Speech.**

Verizon argues that ECPA's record non-disclosure provision is a content-based restriction on speech because one must to look at the content to determine if the restriction applies. Ver.

---

[26] Similarly, the Uniform Trade Secrets Act (UTSA), adopted by most states, prohibits disclosure of a trade secret by one who obtains it through a confidential relationship such as employment, regardless of whether there is an express contract protecting such information. UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 433 (1985). *See, e.g.*, *Expo Chemical Co. v. Brooks*, 572 S.W.2d 8 (Tex. Civ. App. 1978) (explaining that no contract is needed to impose a duty on an employee to refrain from disclosing or using the employer's trade secrets). Information about many trade secrets, which by definition includes new proprietary technologies, would undoubtedly be matters of public concern. Thus, application of state trade secret laws would also be vulnerable to First Amendment challenge.

[27] A number of scholars have persuasively argued that privacy laws and other laws that regulate disclosure of customer information obtained through a business relationship raise no greater First Amendment issue than did the application of a state's promissory estoppel law to a promise by a reporter not to reveal the identity of a confidential source in *Cohen v. Cowles Media*, 501 U.S. 663 (1991). *See, e.g.*, Neil M. Richards, *Reconciling Data Privacy and The First Amendment*, 52 UCLA L. Rev. 1149, 1201-08 (2005). According to these scholars, the non-disclosure statutes are akin to default contract terms that protect the common expectations of the public with respect to the information they provide to banks, lawyers, medical providers, etc.. *Id.* The same would be true with respect to ECPA. However, even if the Court concludes Verizon has a real First Amendment interest in its data disclosure and applies intermediate scrutiny, the most robust form of scrutiny that could possibly apply to the application of ECPA at issue here, it survives that inquiry.

Mem. at 33-34. This formulaic approach is inconsistent with the Supreme Court's repeated assertion that "[d]eciding whether a particular regulation is content based or content neutral is not always a simple task." *Bartnicki,* 532 U.S. at 526 (quoting *Turner Broadcasting, Inc. v. FCC*, 512 U.S. 622, 642-43 (1994)). Indeed, in any number of cases the Supreme Court and Ninth Circuit have held that statutes, which on their face referred to a particular category of speech, were nonetheless content neutral regulations.[28]

The test Verizon sets forth is a *useful* part of the complex inquiry as to whether a restriction is content-based or not, but the inquiry does not end there. Rather, "[t]he government's *purpose* is the controlling consideration." *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (emphasis added); *accord Hill v. Colorado*, 530 U.S. 703, 720 (2000). Content-based laws are subject to more rigorous scrutiny because they "pose the inherent risk that the Government seeks not to advance a legitimate regulatory goal, but to suppress unpopular ideas or information or manipulate the public debate through coercion rather than persuasion." *Turner Broadcasting*, 512 U.S. at 641.

When the government looks at the relevant universe of expression and targets a category of speech of particular content for differential treatment, it raises a red flag that the government has an impermissible purpose. An invalid purpose is less likely with laws that on their face do not discriminate on the basis of content. For example, when a city bans sound trucks in residential neighborhoods after 10 pm, it is likely that the city's purpose is to allow residents tranquility and the opportunity to sleep, not to skew the public debate. If, however, the government asserts the same purpose, but only bans political speech from sound trucks after 10 pm, the court will likely conclude that the real purpose of the ordinance is impermissible. *See Turner Broadcasting*, 512 U.S. at 642. On the other hand, even where the government asserts a content neutral purpose, if close inquiry demonstrates that the asserted purpose is not the *real* purpose, the statute will be treated as content-based. *See id.* The "controlling consideration" is whether the government's purpose stems from disagreement with a particular subject or message. *See id.* at 645. In sum, the purpose inquiry, not Verizon's simplistic test, is the proper means to determine whether a law is content-based. *Ward*, 491 U.S. at 791.

---

[28] *See*, *e.g.*, *Hill v. Colorado*, 530 U.S. 703, 710-20 (2000) (law imposing restrictions on approaching a person "for the purpose of . . . . engaging in oral protest, education, or counseling" not content-based)*; United States v. Kokinda*, 497 U.S. 720, 736 (1990) (four Justice plurality) (restriction on solicitation is content neutral); *id.* at 739 (same) (Kennedy, J., concurring); *Acorn v. City of Phoenix*, 798 F.2d 1260 (9th Cir. 1986) (solicitation ban is content neutral).

ECPA's record non-disclosure provision is content neutral because its purpose is to protect customer privacy and foster private speech, while still allowing for necessary law enforcement access to customer records. S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555 at *3, *5 (purpose is to "protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."). Indeed, this purpose is basically the same one that the *Bartnicki* Court identified as underlying the wiretapping statute, which it held was content neutral. *See Bartnicki*, 532 U.S. at 526 (protecting the "privacy of wire, electronic and oral communications" is content neutral purpose).

Nor is there anything to suggest that Congress' asserted purpose here is pretextual. Congress did not, for example, select out some set of customer records by, for example, allowing disclosure of customer records of any Muslim, that would raise the obvious specter of an invalid government purpose. In short, ECPA is content neutral because the burden on speech it imposes fits neatly with Congress' purpose of protecting customer privacy and fostering private speech. It is unrelated to any "disagreement with the message" that disclosing customer records may convey. *See Hill*, 530 U.S. at 719.

Verizon's approach is more than incorrect, however. It creates a First Amendment "Catch-22" that would make it nearly impossible for legislatures to protect the privacy of customer records. To satisfy Verizon's content neutrality test, and thereby avoid the application of strict scrutiny, the statute would have to bar the disclosure of *all* records, not just those "pertaining to customers." *See* Ver. Mem. at 33-34. Such a statute would prohibit disclosure of an enormous quantity of speech that is entirely *unrelated* to Congress' purpose of protecting customer privacy and fostering private speech, making it unconstitutionally *overbroad*. *See Turner Broadcasting*, 512 U.S. at 662 (content neutral regulations may not "'burden substantially more speech than is necessary to further the government's legitimate interests.'") (quoting *Ward*, 489 U.S. at 799). Either way, then, the statute is doomed.

C. Even If ECPA Is Treated as a Content Based Restriction on Speech, Application of ECPA to Verizon's Massive Disclosure of Customer Records Is Subject to a Balancing Test, or at Most Intermediate Scrutiny.

Even if ECPA *were* treated as content based, its application to Verizon's disclosure of its customers' records would be subject not to strict scrutiny, but to a far more relaxed standard in which the Court balances the competing interests, or at most, applies intermediate scrutiny. Supreme Court precedent—principally *Bartnicki*, 532 U.S. 514, and *Florida Star v. B.J.F.*, 491 U.S. 524 (1989)—requires that result, for two reasons. First, where, speech on the one hand, and privacy—which fosters private speech—on the other hand, are at issue, there are competing interests of the "highest order" that require careful balancing. Second, Verizon's massive turnover of virtually all its customer records is not speech on a matter of public concern.

1. The Customer Records Non-Disclosure Provisions of ECPA Further Privacy, Which In Turn Fosters Private Speech, Both of Which Are Interests of the Highest Order.

In passing ECPA, Congress recognized that enormous advances in communications technology had created the need to update the law to protect against unreasonable infringements on customer privacy. *See* S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555 at *3, *5 ("privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens."); H.R. Rep. 99-647 at 18 (1986) ("[l]egal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology."). Specifically, Congress recognized that telephone customers could have their privacy invaded through technological means of collecting information about the numbers they call. *Id.* at 24. It understood that the realities of modern life had resulted in Americans' losing "their ability to lock away a great deal of personal and business information" which was no longer kept in the home, but instead stored in computer networks maintained by others. S. Rep. 99-541. Congress correctly concluded, however, that "the privacy or proprietary interest in such information should not change" merely because it was in the hands of a third-party. *Id.* It was in this context that Congress enacted additional privacy protections for telephone call records.[29]

---

[29] Congress' recognition of the privacy interests in customer phone records is consistent with that of the FCC. Just recently, the head of the FCC's enforcement bureau testified that "The disclosure of consumers' private calling records represents a significant invasion of personal

Privacy, what Justice Brandeis called the right to be left alone in his seminal dissent in *Olmstead v. United States*, 277 U.S. 438, 478 (1928), is not just a deeply rooted constitutional value for its own sake.[30] Protecting privacy with respect to an individual's communications "foster[s] private speech," which the Supreme Court has recognized as an "interest[] of the highest order." *See Bartnicki*, 532 U.S. at 518; *accord id.* at 536 (Breyer & O'Connor, JJ, concurring). The "assurance of privacy [of communications] helps to overcome our natural reluctance to discuss private matters when we fear that our private conversations may become public." *Id.* at 537 (Breyer & O'Connor, JJ., concurring).

Conversely, "[s]urveillance can make people reluctant to engage in robust and candid discourse. It can inhibit deliberative democracy and individual self-determination. Government information gathering can thus strike at the heart of First Amendment values." Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 1123 (2007). As the Supreme Court stated in *Bartnicki*:

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.

532 U.S. at 533 (quoting President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967)).[31]

Telephone customers use their phones for a wide variety of reasons. However, many of these call are very private, such as calls from patients to their psychiatrists, calls by distraught

---

privacy. *See* Testimony of Kris Anne Montieth, Chief, Enforcement Bureau, FCC, Hearing on "Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?", Sub-Committee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives (September 26, 2006).

[30] The Supreme Court has repeatedly recognized the importance of protecting citizens' privacy. *See, e.g., Florida Star*, 491 U.S. at 532 ("[P]rivacy rights are . . . plainly rooted in the traditions and significant concerns of our society.").

[31] *See also McIntyre v. Ohio Elections, Com'n,* 514 U.S. 334 (1995) (right to anonymous speech in distributing political leaflets); *NAACP v. Alabama*, 357 U.S. 449, 460 (1958) (privacy of membership lists a matter of First Amendment concern); Rodney Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW. U. L. Rev. 1099, 1130 (2002) ("Both speech and association are buttressed by rights to speak and associate anonymously.").

people to suicide hotlines, calls by terrified women to battered women's' shelters, or calls between journalists and confidential sources. If people making these calls believe that they are not confidential, but instead the government has the records and can determine whom they are calling, they will be inclined to self-censor.

2. In Cases Involving Competing Interests in Speech, On the One Hand, and Privacy Which Fosters Private Speech, On the Other, Strict Scrutiny Does Not Apply Where the Disclosure Bar Applies to Speech That is Not of Public Concern.

Ordinarily, when addressing a content-based restriction on speech, the Supreme Court considers whether the restriction satisfies strict scrutiny without first requiring that the speaker demonstrate that the speech involves a matter of public concern. *See, e.g., United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 813 (2000). But when there are *competing* interests of the highest order at stake, as when laws restrict the disclosure of private information, the rule is different. In such cases, particularly where the privacy interest furthers an interest in promoting private speech, an essential part of the legal inquiry is whether the speech is on a matter of public concern. *See Bartnicki*, 532 U.S. at 518, 525; *Florida Star*, 491 U.S. at 536-37. Only then will strict scrutiny even arguably apply. *Florida Star*, 491 U.S. at 532-33, 537.

In *Bartnicki*,[32] the majority opinion never stated explicitly what standard of scrutiny it was applying. *See DVD Copy Control Assn., Inc. v. Bunner*, 31 Cal.4th 864, 879 (2003) (so noting). It did, however, clearly recognize that "there are important interests to be considered on *both* sides of the constitutional calculus," and appeared to engage in a process of balancing the competing constitutional interests in arriving at its holding. *Bartnicki*, 532 U.S. at 533 (emphasis in original); *see id.* ("In considering that balance [between the competing interests], we acknowledge that some intrusions on privacy are more offensive than others, and that disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself."). Justices Breyer and O'Connor, who were also in the majority, expressly recognized the competing interests in speech on the one hand, and protecting privacy and its effect on fostering private speech on the other hand. *Id.* at 536-37. They stated that they favored a balancing approach, rather than applying a more searching inquiry, like strict scrutiny. *See id.* at 537.[33]

---

[32] In *Bartnicki*, the Court considered the application of 18 U.S.C. § 2511, which prohibited the disclosure of the contents of an intercepted conversation by one who knows or has reason to know that the conversation was illegally intercepted. 18 U.S.C. § 2511(c). There, an unknown person illegally intercepted and taped a conversation between Bartnicki, chief labor negotiator for a teacher's union, and Kane, the teacher's union president. The call concerned ongoing labor negotiations, and during the call, Kane indicated that the union might resort to the use of force. The tape was left in the mailbox of Mr. Yocum, who subsequently gave the tape to Vopper, a local radio host, who played the tape on the air. Bartnicki and Kane sued Yocum, Vopper, and other members of the media who had disclosed the contents of the tape, alleging violations of 18 U.S.C. 2511(c) and an analogous state statute.

Similarly, in *Florida Star*, a reporter disclosed the name of a sexual assault victim, in violation of a Florida law prohibiting such disclosures. The facts that the information was both obtained from the government (the name was found in a police report placed by the Sheriff's Department in its press room) and was on a matter of public concern were of key importance. Although faced with a content based restriction, the Court's "first inquiry" was whether the challenged restriction applied to speech that was (1) truthful, and (2) *on a matter of public concern*. 491 U.S. at 536. Only after answering those two questions affirmatively did the Court apply strict scrutiny, and find the statute unconstitutional. *Id.* at 537-41.

Neither the Supreme Court nor the Ninth Circuit has clearly enunciated the level of scrutiny that applies to a content based non-disclosure restriction intended to promote private speech, when the relevant speech is *not* on a matter of public concern. However, it follows *a fortiori* from *Florida Star* that if such a restriction is only subject to rigorous scrutiny where the speech is first determined to be on a matter of public concern, then where it is not, the Court

[33] Both the Stevens and Breyer opinions concluded that because the speech at issue was on a matter of public concern, application of the non-disclosure provisions to *these* defendants—but not to the individual who originally intercepted and then disclosed the information—violated the First Amendment. In their separate concurrence, Justices Breyer and O'Connor made clear that statutory restrictions that protect privacy, by, for example, prohibiting publication of private information, are permissible because of the "importance of these privacy and speech related objectives," so long as the laws are tailored "reasonably to reconcile media freedom with personal, speech related privacy." *Id.* at 537-38. They nonetheless joined the majority opinion because the disclosure of the tape on the radio involved "a matter of unusual public concern." *Id.* at 536-37.

applies, *at most*, some sort of balancing inquiry, as in *Bartnicki*, or intermediate scrutiny.[34] *See Florida Star*, 491 U.S. at 457; *Bartnicki*, 532 U.S. at 534; *id.* at 536 (Breyer, J., concurring). The same holds true here.[35]

As in *Bartnicki*, ECPA's non-disclosure provisions foster private speech by protecting the privacy of customer calling records. Moreover, as we demonstrate below, unlike in *Bartnicki* and *Florida Star*, Verizon's expression is not on a matter of public concern. Thus, strict scrutiny does not apply here.

3. The Disclosure of Verizon's Customer Records Is Not Speech on a Matter of Public Concern.

Plaintiffs are not alleging that Verizon disclosed to the government the customer records of an individual or small group of people whom it believed might be involved in planning terrorist acts. Instead they allege that Verizon disclosed the call records of "*all or substantially all* of their customers, including Plaintiffs"—records for millions of customers whom it knew or should have known had no connection whatsoever to any terrorist threat. MCC ¶¶ 169-170 (emphasis added). These call records are the mundane fabric of daily life. They are not a matter of public concern.

---

[34] This approach—providing robust First Amendment protection only where the speech subject to restriction is on a matter of public concern—is consistent with numerous other areas of First Amendment analysis. For example, courts will only apply the *Pickering* balancing test to restrictions on public employee speech if the court concludes that the speech was on a matter of public concern. *See Connick v. Myers*, 461 U.S. 138, 146 (1983). Similarly, where defamation laws are at issue, the First Amendment protections for speech on a matter of private concern are far less robust than when speech is on a matter of public concern. *See Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759-60 (1985); *id.* at 764 (Burger, C.J., concurring), *id.* at 774 (White, J., concurring).

[35] Verizon is incorrect when it contends that strict scrutiny applies here because its particular speech is intended to influence the government and is therefore political. Ver. Mem. at 32-33. Leaving aside the dubious assertion that turning over millions of customer phone records—records that detail calls made to family members, doctors, as well as pizza parlors—is properly classified as "political speech," Verizon is still incorrect. When determining the appropriate level of scrutiny, the Court looks at the *restriction* at issue—and in this case, the competing constitutional concerns—not the particular *speech* at issue. If the law were as Verizon contends, time, place and manner restrictions would be subject to strict scrutiny whenever the plaintiff alleged that the restriction was affecting its ability to hold a political rally, but would only be subject to intermediate scrutiny if the plaintiff was challenging the restriction as applied to his non-political music festival. That is not the law. *See generally Ward*, 491 U.S. 781.

The Supreme Court recognized the diminished speech interest of a commercial entity like Verizon in the publication of information it obtains from its customers in *Dun & Bradstreet*, 472 U.S. at 761-62; *id.* at 764 (Burger, C.J., concurring); *id.* at 774 (White, J., concurring). The D.C. Circuit has also recognized that disclosure by a consumer reporting agency of consumer reports—business records similar to customer phone records—is not speech on a matter of public concern. *See Trans Union v. Federal Trade Commission (FTC)*, 245 F.3d 809, 818 (D.C. Cir. 2001). In both cases, the courts unequivocally held that a commercial entity that is not a news publication cannot claim full First Amendment protection for the information it includes in a credit report. *See Dun & Bradstreet*, 472 U.S. at 761-62; *id.* at 764 (Burger, C.J., concurring); *id.* at 774 (White, J., concurring). Such speech receives lesser protection because it is "solely in the individual interest of the speaker and its specific business audience." *Id.* at 762.

Similarly, here, whatever interest the government may have in tracking the daily lives of Americans through their phone records, the law does not recognize that information as being of concern to the public. *See Bunner*, 31 Cal. 4th at 883-84 (publication of lawfully obtained trade secret material not of public concern because "only computer encryption enthusiasts are likely to have an interest" in the information (applying *Bartnicki*)). Nor is there any "credible argument" that Verizon's disclosure of customer records to the government "requires special protection to ensure that debate on public issues [will] be uninhibited, robust, and wide-open." *Dun & Bradstreet*, 472 U.S. at 762 (quoting *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)). Because the customer records are not on a matter of public concern, strict scrutiny does not apply here.

D. Under Either a Balancing Inquiry or Intermediate Scrutiny, The Application of ECPA to Verizon's Disclosure of Its Customers' Phone Records Is Permissible.

1. The Interest in Protecting Privacy and Fostering Private Speech Far Outweighs Verizon's Asserted Interest In Turning Over the Records of Millions of Customers to the Government

When a privacy statute, such as the one at issue here, furthers an interest of the highest order—fostering private speech by protecting it from disclosure—and when the information disclosed in violation of the statute—records of the ordinary calls of millions of ordinary individuals—are not on a matter of public concern, the balance tips sharply in favor of the statute's validity. Its undifferentiated disclosure of the call records of millions of innocent people is the polar opposite of disclosure of a single conversation the contents of which not only pertained to a matter of extreme interest to the public, but also explicitly discussed the commission of serious criminal acts. *Compare Bartnicki*, 532 U.S. at 535-36 (Breyer, J. concurring) (Breyer and O'Conner joining majority in holding that application of statute there violates First Amendment because the particular conversation intercepted appeared to involve future criminal conduct and hence was of great public concern), *with Bunner*, 31 Cal. 4^{th} at 883-84 (particular trade secrets disclosed were not of public concern).

The interest in fostering private speech by protecting the privacy of these call records, on the other hand, is particularly strong precisely because of the huge number of records disclosed by Verizon. As the federal government's Office of Technology Assessment concluded in its report, *Electronic Surveillance and Civil Liberties*, in reaching the proper balance between civil liberties and protecting public safety, the scope of surveillance is an important factor to consider. And, where, as here, the surveillance applies to millions of people, it poses a much greater threat to civil liberties than where it is more narrowly focused. *Id.* at 22, Table 6 ("The more people and activities that are subject to surveillance, the more intrusive the surveillance and the greater the threat to our civil liberties."). Further, the lower the level of individualized suspicion, the less public safety justification there is for intrusions on privacy. *Id.* The dragnet programs alleged are the very antithesis of individualized suspicion.

This conclusion is consistent with the Framers' concern about general warrants, and the longstanding constitutional norm that dragnet or mass searches or seizures, as opposed to those based on some kind of individualized suspicion, are unreasonable. *See Payton*, 445 U.S. at 583 ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."); *Carroll v. United States*, 267 U.S. 132, 153-54 (1925) ("It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search."); *see also City of Indianapolis v. Edmond*, 531 U.S. 32 (2000) (holding drug interdiction checkpoints unconstitutional).

In sum, the interest in promoting private speech furthered by ECPA far outweighs Verizon's asserted justifications for the wholesale turnover of its customers' records. Nevertheless, Verizon contends that its actions are entitled to *more* First Amendment protection than the disclosure of the taped conversation in *Bartnicki*. That claim is wrong for three reasons.

First, Verizon omits an important factor in contending that the records here were obtained in the lawful course of business: Verizon voluntarily placed itself in a position to obtain records here, knowing that there was a statutory duty of confidentiality, to which Verizon also added a contractual duty in its privacy policy. Specifically, that policy states:

> **Your Telephone Account Information Rights**
>
> The FCC refers to your telephone account information as Customer Proprietary Network Information or CPNI. *Under Federal Law, you have the right to, and we have the duty to protect, the confidentiality of your telecommunications service information. This information includes the type, technical arrangement, quantity, destination, and amount of use of telecommunications services and related billing for these services.*

Verizon Telephone Company Customer Privacy, "Your Telephone Account Information Rights," *available at* http://www22.verizon.com/about/privacy/customer/.

Thus, Verizon's interest in unrestricted disclosure is far less than defendants' in *Bartnicki*, who had not voluntarily placed themselves in a position that would subject them to disclosure restrictions. *See Aguilar v. United States*, 515 U.S. 593, 605 (1995) ("As to one who voluntarily assumed a duty of confidentiality, governmental restrictions on disclosure are not subject to the same stringent standards that would apply to efforts to impose restrictions on unwilling members of the public."); *American Motors Corp. v. Huffstutler*, 575 N.E.2d 116, 120 (Ohio 1991) (enforcing attorney client privilege against person who voluntarily submits to state licensing to be an attorney does not violate the First Amendment).

Second, one of the lynchpins of the majority's reasoning in *Bartnicki* was that the principal method to protect privacy under these circumstances would be to punish the third party who illegally intercepted the communication rather than punishing the speech of the media, which had not engaged in the illegal interception. *Bartnicki*, 532 U.S. at 529-30. Here, there is no third party to be regulated. If Congress wants to preserve the confidentiality of the information, it must regulate Verizon's conduct, since it is the entity that possesses the records. *See also Trans Union v. FTC* (*Trans Union II*), 267 F.3d 1138, 1142 (D.C. Cir. 2001) ("The government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent.").

Third, Defendants err in contending that, because the disclosure here was only to the government, it is more clearly protected than the speech at issue in *Bartnicki*. This contention pays scant heed to the real threat posed by unauthorized government surveillance in the modern age. Indeed, the most chilling literary depiction of loss of privacy, George Orwell's *1984*, concerns the *government's* ability to exercise total control of the population by monitoring every facet of citizens' private lives. While *1984* is a fictional work, modern history is littered with examples of improper and unreasonable government surveillance. *See* Richards, *Reconciling Data Privacy*, 52 UCLA L. Rev. 1149, 1158 (2005). Our foundational guarantee of personal liberty, the Bill of Rights, protects individuals *only* against the excesses of government, further belying Verizon's assertion that the harms from improper government surveillance are minimal.

2. **Application of ECPA to Verizon's Disclosure of the Records of Millions of Its Customers Easily Satisfies Intermediate Scrutiny.**

Defendants' First Amendment argument also fails if the Court concludes that intermediate scrutiny is the proper standard. Intermediate scrutiny requires that application of ECPA be narrowly tailored to satisfy a substantial government interest. *Turner Broadcasting*, 512 U.S. at 662. The requirement of narrow tailoring does not require that the legislature find the perfect means of effectuating its goal. It is sufficient that the means chosen "do not burden substantially more speech than is necessary to further the government's legitimate interest." *Id.*

As explained above, protection of customer privacy and the consequential fostering of private speech is an interest of the "highest order," and therefore more than sufficient to satisfy the "substantial interest" test. *See Bartnicki*, 532 U.S. at 518, 532; *see also Trans Union*, 245

F.3d at 818 ("[W]e have no doubt that this interest—protecting the privacy of consumer credit information—is substantial.").

Narrow tailoring is achieved by Congress' limitation of the reach of ECPA's non-disclosure provision solely to customer records, rather than including information Verizon collects that does not affect customers' privacy. Verizon's assertion that ECPA is overbroad because it could have achieved its purposes by limiting the *uses* the government might make of the information ignores the fact that a customer's privacy in his phone records is undermined by disclosure alone. *See Trans Union II*, 267 F.3d at 1142 ("the government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent."). The fact that a customer's privacy might be *further* injured by misuse of the information by the government does not render limitations on the initial disclosure invalid.

Nor is ECPA impermissibly underinclusive. First, Verizon is wrong when it claims that because ECPA applies only to disclosures of records to the government, it does not effectively protect privacy. ECPA must be viewed in the larger framework of federal protection for customer call records. Other provisions of federal law protect customer privacy by prohibiting the phone companies from disclosing customer records to non-governmental entities. Specifically, 47 U.S.C. § 222(c) imposes a "duty" on the phone companies to protect the privacy of "customer proprietary network information" (CPNI), prohibiting the disclosure of those records to anyone except in certain narrowly delineated circumstances.

Second, Verizon's discussion of the non-disclosure exceptions in ECPA is premised on the applicability of strict scrutiny, which requires a near-perfect fit between purpose and result; underinclusiveness can be fatal. Where, as here, strict scrutiny does *not* apply, "[t]he primary purpose of underinclusiveness analysis is to 'ensure that the proffered state interest actually underlies the law, [so] a rule is struck for *under* inclusiveness only if it cannot fairly be said to advance any genuinely substantial governmental interest because it provides only ineffective or remote support for the asserted goals, or limited or incremental support." *Trans Union*, 245 F.3d at 819. ECPA directly and effectively addresses Congress' asserted purpose of protecting the privacy of customer records, while at the same time providing clear exceptions whereby the government may obtain information and the phone companies may make disclosures for public safety purposes. *See* S. Rep. 99-541 at *3, *5, 1986 U.S.C.C.A.N. 3555.

Nor is ECPA impermissibly underinclusive because it allows the government to obtain records through administrative subpoena, *see* 18 U.S.C. § 2703(c)(2), or permits phone companies voluntarily to disclose records that relate to a report to the National Center for Missing and Exploited Children (NCMEC), *see* 18 U.S.C. § 2702(c)(5). Ver. Mem. at 38, 40. It is not that preventing terrorism is any less important than preventing the exploitation of children or furthering administrative investigations. The problem with Verizon's argument is that Congress limited its exceptions to instances involving a concrete nexus between the limited disclosure of records and the crime or other problem sought to be addressed.[36] That distinction does not render ECPA unconstitutional. In fact, that distinction is fundamental to a free society built on the rule of law and the requirement of individualized suspicion. *See generally* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev.1083, 1109 (2002) ("Particularized suspicion keeps the government's profound investigative powers in check preventing widespread surveillance and snooping into the lives and affairs of all citizens.").

E. The Petition Clause Does Not Immunize Verizon's Disclosure of Its Customer Records to the Federal Government.

Verizon's claim that disclosure of its customer call records constitutes activity protected under the Petition Clause misapprehends the nature of that protection. The First Amendment guarantees "the right of the people ... to petition the Government for a redress of grievances."

[36] For example, ECPA allows a disclosure of records without customer approval in connection with a report to NCMEC under 42 U.S.C. § 13032. 18 U.S.C. § 2702(c)(5). Section 13032 in turn requires reporting to NCMEC by a phone company that "obtains *knowledge of facts and circumstances* from which a violation of [laws prohibiting the sexual exploitation of children] involving child pornography is *apparent*." 42 U.S.C. § 13032(b) (emphasis added). Permitting disclosure of a record where a phone company has that level of individualized suspicion is a far cry from allowing the disclosure of the phone records of millions of innocent customers based on no individualized suspicion whatsoever. Similarly, allowing disclosures where the government certifies that specific records are *relevant* to an authorized investigation (*see, e.g.*, 15 U.S.C. 77s(c) (authorizing SEC to issue subpoenas where material sought is relevant or material to enforcement of the law)) does not either undermine the importance of Congress' interest in protecting privacy, or require that Verizon be allowed indiscriminately to infringe on the privacy of millions of its customers.

U.S. Const., Am. I. The purpose of the clause is to protect the right of the people to "use the channels and procedures of state and federal agencies and courts to advocate their causes and points of view." *California Motor Transport Co. v. Trucking Unlimited*, 404 U.S. 508, 511 (1972); *see also Eastern R. R. Presidents Conference v. Noerr Motor Freight, Inc.*, 365 U.S. 127, 137 (1961).

Verizon's argument under the Petition Clause stalls at the starting gate because Verizon cannot show that ECPA in any way inhibits its ability to petition for redress of grievances or "to advocate [its] causes and points of view." *Trucking Unlimited*, 404 U.S. at 511. The provision at issue here, 18 U.S.C. § 2702(c), only prohibits Verizon's disclosure of its customers' records. Its restrictions do not stop Verizon from telling the government of its concerns about terrorism; its belief that its records might be used to help identify terrorists; general facts about the nature, extent and format of its database of customer records; legal means by which Verizon might turn over the records; or Verizon's belief that changes in the law are necessary to bring such legal means about. While Verizon may affirmatively request that the NSA take legal action to permit the examination of Verizon's customer records, the records themselves are neither a request nor information necessary for the government to evaluate that request.

Further, while Verizon may think it important for the government to examine its customers' records—which flies in the face of its public assurances of their protection—"[a] citizen's right to petition the government does not guarantee a response to the petition or the right to compel government officials to act on or adopt a citizen's views." *Apple v. Glenn*, 183 F.3d 477, 479 (6th Cir. 1999); *see also Smith v. Arkansas State Highway Emp., Local 1315*, 441 U.S. 463, 465 (1979). The Petition Clause would allow Verizon to advocate for action prohibited by ECPA, *see White v. Lee*, 227 F.3d 1214, 1227 (9th Cir. 2000), but a legal prohibition against the relief sought does not violate the Petition Clause.

Nor is this a case about Verizon informing the government about, or requesting government action concerning, any specific unlawful act of any of its customers. Here, Verizon is alleged to have divulged vast amounts of information, at the direct request *of* the government, without any specific knowledge of wrongdoing at all and with full knowledge that the overwhelming majority of the records would concern law-abiding customers. The cases cited by Verizon that find some measure of protection for reporting suspicions to law enforcement uniformly concern reports of specific allegations of particular unlawful acts.[37] Any protection the Petition Clause provides for reporting specific unlawful acts does not extend to the wholesale disclosure Verizon engaged in here, over the directly contrary instructions of Congress.

Similarly, Verizon gains no additional protection by treating the issue as involving petition rather than speech. The Supreme Court has recognized that "[a]lthough the right to petition and the right to free speech are separate guarantees, they are related and generally subject to the same constitutional analysis." *Wayte v. United States*, 470 U.S. 598, 611 n.11 (1985); *accord Rendish v. City of Tacoma*, 123 F.3d 1216, 1220-22 (9th Cir. 1997). The Court has firmly rejected the idea that the Petition Clause affords greater protections than the speech clause. *McDonald v. Smith*, 472 U.S. 479, 482-85 (1985) ("no sound basis for granting greater constitutional protection to statements made in a petition to the President than other First Amendment expressions"). Verizon offers no case, and plaintiffs are aware of none, holding that a communication to government, outside the initiation of a formal proceeding, would find protection under the Petition Clause not conferred by the Speech Clause.

Verizon's assertion that the *Noerr-Pennington* doctrine must be applied to provide "breathing space" for its otherwise unlawful actions is flawed in two core respects. First, although it finds its roots in the First Amendment, *Noerr* is not an absolute immunity, but an application of the constitutional avoidance doctrine. It thus requires that statutes be read narrowly to prevent impinging on advocacy for government action, thereby avoiding constitutional questions. *See, e.g., BE & K Const. Co v. NLRB*, 536 U.S. 516, 535 (2002); *Sosa v. DIRECTV, Inc.*, 437 F.3d 923, 931 (9th Cir. 2006).[38] Verizon points to no case where the doctrine has been

[37] *See, e.g., Forro Precision, Inc. v. IBM Corp*, 673 F.2d 1045, 1050-52, 1060 (9th Cir. 1982) (reporting to police suspicions that plaintiff had stolen trade secrets); *King v. Idaho Funeral Serv. Ass'n*, 862 F.2d 744, 745 (9th Cir. 1988) (reporting that caskets were being sold without required license); *Quarles*, 158 U.S. at 535-36 (informing deputy marshal petitioner was distilling liquor without license).

[38] *Sosa* made clear that the *Noerr-Pennington* doctrine is not a direct immunity from liability clearly imposed by a statute, but an application of the canon of avoidance, under which courts "construe federal statutes so as to avoid burdening conduct that implicates the protections afforded by the Petition Clause *unless the statute clearly provides otherwise*." *Sosa v. DIRECTV,*

applied to confer immunity for disclosures that fell squarely within a narrowly drawn and otherwise valid statutory prohibition. Here, the text of ECPA explicitly bars disclosure of consumer records to the government, making Congress' intent to prohibit communication of this information patently clear. *See* 18 U.S.C. § 2702(c). The courts may not create ambiguity where none exists. Defendants' attempt to turn a canon of statutory construction into an immunity lacks any foundation.

Second, the "breathing space" given under *Noerr-Pennington* is simply an application of the general First Amendment principles that (1) "certain classes of speech not meriting protection in themselves – the false statements in *New York Times*, for example – must nevertheless be protected in order fully to vindicate the free speech rights guaranteed by the First Amendment;" and (2) "certain conduct, not in itself speech, is protected in order adequately to protect the actor's ability to exercise his free speech rights." *Sosa*, 437 F.3d at 933-34. The first category is generally invoked only in defining the scope of *Noerr-Pennington*'s "sham" exception (for petitions that use a lawful process for unlawful purposes), while the second has been applied to limit the reach of statutes to communications with private actors that, while not petitions themselves, are required to organize for effective petitioning. *See id*. at 934. Neither of these principles is relevant here, as the disclosures are not alleged to be "sham" and were not to private actors.

Verizon's claim that its disclosures are deserving of greater protection because of the discretion exercised by the NSA, Ver. Mem. at 31, relies on inapplicable language taken out of context. The discretion of the agency involved is relevant to the scope of *Noerr-Pennington*'s "sham" exception, because the greater the discretion of the agency—and the fewer the procedural constraints that bind it—the less meaningful the concept of a "baseless" petition. *See Kottle*, 146 F.3d at 1062. Such discretion is irrelevant here where plaintiffs do not allege Verizon's

---

Inc., 437 F.3d 923, 931 (9th Cir. 2006) (emphasis added). The Ninth Circuit's conclusion in *Sosa* was based on the Supreme Court's analysis in *BE & K*, and supersedes earlier, broader dicta about the nature of *Noerr-Pennington*. *Cf. Kottle v. Northwest Kidney Centers*, 146 F.3d 1056, 1059 (9th Cir. 1998).

disclosure were a "sham," but rather (1) that the disclosures were not petitions, and (2) that the clear mandate of ECPA prohibiting the disclosures neither requires, nor is susceptible to, a narrowing construction under *Noerr-Pennington*'s canon of avoidance.[39]

Finally, Verizon distorts the case law by suggesting its actions are protected by an implied "fundamental constitutional right" to assist the government. The Supreme Court in *In re Quarles*, 158 U.S. at 535-36, recognized the right to inform a government of violations of its laws as an inherent feature of citizenship.[40] It interpreted a federal statute penalizing conspiratorial threats against a citizen's exercise of "any right or privilege secured to him by the constitution or laws of the United States," as being applicable to a retaliatory assault on a citizen who had informed federal authorities about violations of federal law. *Id.* at 535. But this privilege has never been afforded the status of a constitutional right sufficient to invalidate a federal statute.[41] Indeed, the Supreme Court, while acknowledging *Quarles* for its general principle that informing should be encouraged, not punished, has held that informing on federal immigration violations may be penalized as an unfair labor practice. *See Sure-Tan, Inc. v. NLRB*, 467 U.S. 883, 896 (1984). Even if it were wise to provide the protection of federal statutes to those who inform government of unlawful activity, as in *Quarles*, or common law tort privileges against liability, *see* Res. (2d) Torts § 139(2), there exists no implied constitutional right that limits Congress' power to enact

[39] Contrary to Verizon's claim here, courts addressing the scope of the sham exception have found that police have less discretion than legislatures, and that *Noerr-Pennington* accordingly provides much narrower protection to complaints to law enforcement than to legislative petitioning. *See Kottle*, 146 F.3d at 1062 ("We have suggested that the sham exception is narrower in communications with the police than it is in the legislative realm.").

[40] The cases cited by Verizon "affirming" *Quarles* simply mention informing the government of unlawful acts in passing *dicta* as an example of one of the small number of privileges and immunities inherent in national citizenship. *See Chapman v. Houston Welfare Rights Organization*, 441 U.S. 600, 613 (1979) (referring in passing to *Quarles* as example of rights protected, but not created, by Constitution under Revised Statute § 5508 (currently 18 U.S.C. § 241); *In re Sacred Heart Hosp.*, 133 F.3d 237, 244 n.11 (3d Cir. 1998) (in rejecting argument for right to bankruptcy under Privileges and Immunities clause, listing informing of unlawful acts as one of few recognized privileges and immunities).

[41] Indeed, *Quarles*' interpretation of the statute at issue was based largely on federalism concerns—that leaving the state to punish conspiracies against enforcement of federal laws would undermine the national government. 158 U.S. at 536-37. These concerns are not present where, as with ECPA, it is Congress, not a state, that has restricted disclosure to federal authorities.

laws that limit wholesale disclosure of private information and are otherwise valid under the First Amendment.

F. The Doctrine of Constitutional Avoidance Does Not Require That The Court Rewrite ECPA.

Verizon's contention that the doctrine of constitutional avoidance requires this Court to interpret the "emergency" and "rights of property" exceptions in ECPA to apply to their massive disclosure is unfounded for three reasons. First, "the canon of constitutional avoidance has no application in the absence of statutory ambiguity." *United States. v. Oakland Cannabis Buyers' Co-op*, 532 U.S. 483, 495 (2001). As Plaintiffs explained in Part II, it would be inconsistent with the statutory language and congressional intent to interpret either of those exceptions to apply to Verizon's disclosure.

Second, even if Verizon's interpretation of ECPA's exceptions were a reasonable one, its First Amendment argument is not sufficiently persuasive to raise the "grave doubts" that would prompt the Court to apply the constitutional avoidance doctrine here. *United States v. Jim Min Fuey*, 241 U.S. 394, 401 (1916); *accord Almendarez-Torres v. U.S.*, 523 U.S. 224, 238-39 (1998).

Finally, as Plaintiffs have explained above, in this case, there are competing constitutional concerns in speech on the one hand, and privacy which fosters private speech on the other. If the Court were to read the ECPA exceptions broadly in order to protect Verizon's asserted First Amendment interests, it would be harming the First Amendment interests of Verizon's customers, which ECPA protects. Thus, the very act of constitutional avoidance that Verizon encourages would minimize the constitutional interests that Congress intended to protect. Rewriting ECPA in a manner that undermines its very purpose and does violence to the plain meaning of its terms is neither justified nor permissible here.

VII. PLAINTIFFS' STATE LAW CLAIMS ARE WELL PLEADED, AND VERIZON'S SWEEPING PREEMPTION THEORIES ARE UNFOUNDED.

A. Federal Law Does Not Preempt Plaintiffs' State Law Claims.

Notwithstanding the well-pleaded allegations that Verizon disclosed Plaintiffs' communications and records without statutory authorization or certification, MCC ¶ 177, and not to protect Defendants' property nor because an emergency involving death or serious physical injury required immediate disclosure, MCC ¶ 182, Verizon insists that Plaintiffs' state law claims are preempted as "statutorily authorized by the 'emergency' and 'property rights' exceptions" of ECPA. Ver. Mem. at 46. Defendants here confuse express federal preemption of state law claims with a potential, albeit implausible, statutory defense they might assert at trial. In any event, as explained in Part II, *supra*, these statutory exemptions are not even remotely applicable to the conduct alleged.

Defendants provide no authority that even *hints* that Congress expressly intended the "emergency" and "property rights" exceptions to preempt Plaintiffs' state law claims. *See English v. General Elec. Co.*, 496 U.S. 72, 79 (1990) (express preemption occurs only where Congress "define[s] explicitly the extent to which its enactments pre-empt state law"). Defendants all but ignore this Court's holding, in this same litigation, "that [ECPA] does not completely preempt suits under state law." *In re NSA Telecoms. Records Litig.*, 483 F. Supp. 2d. 934, 939 (N.D. Cal. 2007). Verizon's express preemption argument goes nowhere.

Alternatively, Defendants refer to the Court to their "constitutional field preemption" argument, put forward in their motion to dismiss the *Riordan, Bready, and Chulsky* Complaints (Dkt. No. 271), Ver. Mem. at 46, which essentially says that since "national security" is "a field entrusted to the federal government," Plaintiffs' state law claims are preempted because, Defendants say, they involve national security. *Id.* As already noted by the Court in rejecting an earlier version of Defendants' preemption argument, "defendants' repeated invocation of the 'sweeping authority of Congress and the Executive' to protect national security misses the mark." *In re NSA Telecoms. Records Litig.*, 483 F. Supp. 2d at 939 (rejecting application of "doctrine of complete preemption").[42] Plaintiffs' state law privacy claims neither implicate foreign affairs nor directly regulate the federal government, but rather are consonant with, and complimentary to, Congressional statutes that expressly contemplate concurrent state regulation of electronic surveillance. *See id*. at 940-41 ("FISA thus contemplates that, in the absence of a government order for business records under 50 USC § 1861(a)(1) (as alleged here), injured parties will have causes of action and remedies under other provisions of state and federal law. . . . [T]he California laws on which plaintiffs' claims are based do not make unlawful an act of defendants that federal law or policy deems lawful.").

---

[42] For all of the reasons set forth in Plaintiffs' Joint Opposition to Verizon's Motion to Dismiss the *Chulsky, Riordan, and Bready* Complaints (Dkt. No. 304 at 11-19), which Plaintiffs hereby adopt and incorporate by reference, Defendants' "constitutional preemption argument" is groundless and literally unprecedented.

B. Plaintiffs' State Law Claims Satisfy Notice Pleading Standards.

By alleging that Verizon and MCI falsely and knowingly represented that they would not disclose their customers' communications and records without their consent or a court order, when in fact Verizon and MCI were disclosing their customers communications and records to the NSA without their consent or a court order, Plaintiffs have given Defendants ample notice of the facts underlying their breach of contract and statutory consumer protection claims. *See* MCC ¶¶ 177-181, 268-69, 274-75.

Plaintiffs specifically allege that Verizon and MCI, through "privacy policies falsely assure[d] Plaintiffs [and] Class Members that information pertaining to their telephone calls and/or electronic communications will not be disclosed to third parties absent a valid court order or subpoena." MCC ¶ 268; *see also* MCC ¶¶ 179-180 (quoting Verizon policies as "example" of privacy policy violated). These allegations are specific enough to give Defendants ample notice to respond to Plaintiffs' claims, especially as Defendants are well aware of their own customer privacy policies, and how they violated those policies.

"Notice pleading does not impose heightened pleading standards when alleging a breach of contract." *Chaganti v. 12 Phone Int'l Inc.*, No. 04-CV-0987, 2005 WL 679664, at *3 (N.D. Cal. March 11, 2005) (Walker, J.). Despite this well-settled law, Verizon insists that Plaintiffs' claims for breach of Defendants' privacy policies must be dismissed because the "Complaint does not allege that the privacy policies, which are quoted, were incorporated into any contracts with Verizon." Ver. Mem. at 48. Plaintiffs need not plead the specific text in Verizon's subscriber contracts incorporating Verizon's privacy policies, but rather "plead it according to its effect." *Northwest Pipe Co. v. Travelers Indem. Co.*, No. 02-CV-04189, 2003 U.S. Dist. LEXIS 26416, at

*10, 2003 WL 24027882, at * 3 (N.D. Cal. Feb. 12, 2003). Here, by alleging as an element of their breach of contract and consumer protection claims that "Defendants impliedly and expressly promised to protect the privacy and confidentiality of their customers' information, identity, records, subscription, use details, and communications," MCC ¶ 274, and by quoting examples of privacy policies breached, MCC ¶¶ 179-180, Plaintiffs have sufficiently pleaded the contracts' effect, as to both Verizon and MCI.[43]

For the same reason, Defendants' argument that Plaintiffs' breach of contract and consumer protection claims as to defendant MCI must be dismissed because "Plaintiffs do not cite any MCI privacy policies" is unsound. Ver. Mem. at 47. Plaintiffs have sufficiently alleged the material terms of MCI's privacy policies. *See, e.g.*, MCC ¶ 268. Plaintiffs need not attach or quote a contract to satisfy notice pleading standards. *Bicoastal Corp. v. Aetna Cas. And Sur. Co.*, No. C-94-20108, 1994 WL 564539, at *3 (N.D. Cal. Oct. 4, 1994) (citing *Venture Assoc. Corp. v. Zenith Data Systems Corp.*, 987 F.2d 429, 431 (7th Cir. 1993) ("A plaintiff is under no obligation to attach to her complaint documents upon which her action is based.")).

Finally, Verizon argues that plaintiff Spielfogel-Landis' claims for violation of Verizon's privacy policies subsequent to its acquisition of MCI fails to state a claim, because she has not specifically alleged that she "enter[ed] into a new service agreement with Verizon . . . ." Ver. Mem. at 47. This is patently absurd. Since at least November 2005—two months before its acquisition of MCI—Verizon's "Privacy and Customer Security Policies," which remain posted on its website, expressly assure customers of *all* of its subsidiaries, *including* MCI, that "Each Verizon company is responsible for implementing these Principles," which include:

> Subject to legal and safety exceptions, Verizon will share individual customer information only with persons or entities outside the company when the customer has consented, or when we have advised the customer of the opportunity to "opt-out" (to choose not to have the information disclosed).

Privacy and Customer Security Policies, Disclosure of Individual Customer Information

---

[43] *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196 (D.N.D. 2004), cited by Verizon in support of its argument, holds only that "broad statements of company policy do not generally give rise to contract claims," and characterizes the policy at issue as "[in]sufficiently definite." *Id*. at 1200. By contrast, the privacy policies alleged in this case are clear and precise.

(November 2005) (available at http://www22.verizon.com/about/privacy/genpriv/#10).[44]

VIII. THE CLAIMS AGAINST MCI ARE NOT BARRED BY MCI'S BANKRUPTCY DISCHARGE.

Verizon takes the extraordinary position that the claims against MCI are barred by orders entered in MCI's 2002 bankruptcy case, even though: (1) the claimants did and *could not have* known of the existence of their claims at the time of the bankruptcy; (2) no notice of their claims or the relevant bankruptcy bar dates was provided; and (3) many of the claims arise from *post*-bankruptcy activities of MCI. Verizon's assertions are patently frivolous.

As set forth in the Master Complaint, Plaintiff Spielfogel-Landis was a customer of MCI prior, during, and subsequent it Chapter 11 bankruptcy. *See* MCC ¶ 8. She had no idea that MCI had granted the NSA access to her call contents and records. *See id.* ¶ 240. She asserts that each act of MCI providing access to a customer's call content and records after September 11, 2001 (up to January 6, 2006) created a separate and distinct claim.

MCI filed its Chapter 11 petition in 2002, and confirmed a Chapter 11 plan in 2003. *See* Ver. Mem. at 49. Verizon maintains that MCI's actions gave rise to "claims" under § 101(5) of the Bankruptcy Code, and that the confirmation order bars not only the pre-petition claims, and claims arising throughout the Chapter 11 case, but also the claims arising post- confirmation. *See id.* at 48-49. Verizon does not allege that MCI listed the pre-petition claims of Spielfogel-Landis in its bankruptcy schedules; that it notified her that she had a claim that might be affected by its bankruptcy case; or that it provided Landis with mailed notice of the bar date for the filing of proofs of claim, or of the confirmation of its plan. Even if this Court were to consider Verizon's arguments in the context of a motion to dismiss,[45] they are totally without merit, and must be rejected.

---

[44] Indeed, Verizon attaches a version of these principles specific to its wireless division as Exhibit 1 to its request for judicial notice in support of its motion to dismiss. In the event that the Court finds that Plaintiffs' allegations do not give Verizon sufficient notice of Plaintiffs' state law claims, Plaintiffs respectfully request leave to amend the Master Complaint to make additional allegations. *See Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1051 (9th Cir. 2003) (leave to amend under Rule 15 is "to be applied with extreme liberality").

First, it is a fundamental principle of law that "the protections afforded by discharges from bankruptcy are not meant to extend to viable claims against debtors who [like MCI] did not provide notice to claimants." *In re Conseco Life Ins. Co. Cost of Insurance Litigation*, 2005 WL 2203150, *7 (C.D. Cal. 2005) (*citing In re Savage Industries, Inc.*, 43 F. 3d 714, 719-721 (1st Cir. 1994)). Thus, before a debtor can obtain a discharge of a claim in a Chapter 11 bankruptcy, due process requires that the claimant receive notice of the bankruptcy case and the applicable bar date, so that creditors have an opportunity to participate and make claims in the bankruptcy. *Monster Content, LLC v. Homes.Com, Inc.*, 331 B.R. 438 (N.D. Cal. 2005); *In re XO Communications*, 301 B.R. 782 (Bankr. S.D.N.Y. 2003). If a Chapter 11 debtor does not give actual notice to a known creditor of the bankruptcy proceeding and the applicable bar date, that creditor's claim is not discharged and the creditor's suit can proceed. *In re Maya Construction Company*, 78 F.3d 1395, 1399-1400 (9th Cir. 1996); *In re Chemetron Corp.*, 72 F.3d 341, 345 (3rd Cir. 1995); *Monster Content*, 331 B.R. at 443. A Chapter 11 creditor who is not provided notice, *even if it has actual knowledge of the reorganization*, does not have a duty to investigate, or inject itself into the reorganization proceedings. *Maya Construction Co.*, 78 F.3d at 1399; *Monster Content*, 331 B.R. at 443; *XO Communications*, 301 B.R. at 792 n.5.

Second, "nothing in the legislative history or the [Bankruptcy] Code suggests that Congress intended to discharge a creditor's rights before the creditor knew or should have known that its rights existed." *In re Hexcel Corp.*, 239 B.R. 564, 567 n.3 (N.D. Cal. 1999) (quoting *In re Jensen*, 995 F. 2d 925, 930 (9th Cir. 1999)); *accord In re Conseco Life Ins. Co. Cost of Ins. Litig.*,

---

[45] The Federal Rules of Civil Procedure expressly require that the defense of "discharge in bankruptcy" be raised by a defendant as an affirmative defense, not in a motion to dismiss. Rule 8(c), Fed. R. Civ. P.

2005 WL 2203150 (C.D. Cal. 2005) (holding that a breach of contract claim was not barred by Conseco's Chapter 11 case, even though plaintiffs, unlike Spielfogel-Landis, received actual knowledge that a breach *might* occur several weeks prior to the discharge order).

Because Spielgofel-Landis did not know and *could not have known* about the surreptitious conduct of MCI until the press coverage in late 2005-early 2006, her claims are not barred. This is unlike the facts in *Jensen*, where both the claimant (the California Dept. of Health Services) and the debtor knew of the environmental contamination prior to the filing of the bankruptcy case. *Jensen*, 995 F.2d at 931. The Ninth Circuit adopted a "fair contemplation" test in *Jensen*, finding that the existence of the possible environmental claim was fairly contemplated by the parties. Applying the test enunciated by the Ninth Circuit's in *Jensen*, Spielfogel-Landis' claims against MCI were simply not within her "fair contemplation" in 2002 or 2003. *Id*. at 930. Indeed, Verizon argues that the very existence of her claims is an unknowable "state secret."

Finally, Verizon argues that MCI's continued participation in the NSA programs after the petition date, and after the confirmation date of MCI's plan, does not give rise to new claims, but merely to a continuation of the pre-discharge claims, which, in Verizon's view, are discharged. Obviously, this argument fails because the pre-discharge claims are *not* barred, for the reasons set forth above. Even assuming, *arguendo*, that the pre-discharge claims *were* barred, controlling Ninth Circuit authority, *O'Loghlin v. County of Orange*, 229 F.3d 871 (9th Cir. 2000), disposes of this argument. In *O'Loghlin,* the court held that the continuing wrongful course of conduct of a defendant post-discharge does not relate back to the defendant's wrongful pre-discharge conduct such that the defendant may avoid liability for later illegal conduct of the same sort. *Id.* at 875.[46]

---

[46] The Ninth Circuit stated, "The bankruptcy laws provide no justification for such a result. Their purpose is to provide a 'fresh start' to a discharged debtor… A suit for illegal conduct occurring after discharge threatens neither the letter nor the spirit of the bankruptcy laws. A 'fresh start' means only that; it does not mean a continuing license to violate the law." *Id.*

Like the debtor in *O'Loghlin*, MCI was not given a "continuing license to violate the law," and the claims arising post-discharge were not discharged.

Verizon cites to *In re Hassanally*, 208 B.R. 46, 47 (9th Cir. BAP 1997), and two *WorldCom* opinions, one of which was reversed on appeal. Unlike the present case, in *Hassanally,* all of the defective construction work occurred pre-petition, so that case says nothing about the circumstances present here.[47] In both *In re Worldcom, Inc*., 320 B.R. 772 (Bankr. S.D.N.Y. 2005), and *In re Worldcom, Inc.*, 328 B.R. 35 (Bankr. S.D.N.Y. 2005), the bankruptcy court interpreted state laws to determine whether the allegedly improper *pre-petition* installation of fiber optic cables on railroad easements adjoining the plaintiffs' real property constituted a "permanent trespass" or a "continuing trespass." The bankruptcy court found that any trespass was a permanent trespass occurring pre-petition since no new cable was installed post-petition. On appeal, however, the district court reversed the bankruptcy court's ruling in 328 B.R. 35, because of the debtor's future need to trespass on the plaintiffs' property to maintain and repair the cable. *See West v. Worldcom, Inc.*, 2007 WL 485233 (S.D.N.Y. 2007). These post-discharge trespasses, like MCI's wrongful post-discharge participation in the NSA programs, were not affected by MCI's bankruptcy case.[48]

---

[47] In *Hassanally*, a Chapter 7 no asset case, the debtor listed a secured creditor in his schedules, providing notice to the creditor of the bankruptcy filing. Subsequently, the creditor asserted a claim for defective construction in connection with the property securing its claim, defects which the court held were within the "fair contemplation" of the creditor. *Hassanally*, 208 B.R. at 51, 55. The narrow, fact-based holding of *Hassanally* was emphasized in *In re Hexcel Corp.*, 239 B.R. 564, 569 (N.D.Cal. 1999).

[48] The remaining cases cited by Verizon are Chapter 7 cases that provide no support to Verizon. *See, e.g., In re Conseco*, 2005 WL 2203150, at 6 (discussing narrow scope of *In re Russell*, 193 B.R. 568, 571 (Bankr. S.D. Cal. 1996), a Chapter 7 no asset case); *In re Emelity*, 251 B.R. 151 (Bankr. S.D. Cal. 2000) (claims of Chapter 7 debtor's ex-wife, who received notice, were determined to be within the "fair contemplation" of the parties and thus discharged).

CONCLUSION

For the reasons set forth above, the Court should deny Verizon's Motion to Dismiss.

Dated: June 22, 2007

Respectfully submitted,

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP

By: *\s\ Barry R. Himmelstein*
Barry R. Himmelstein

Elizabeth J. Cabraser (State Bar No. 083151)
Barry R. Himmelstein (State Bar No. 157736)
Michael W. Sobol (State Bar No. 194857)
Eric B. Fastiff (State Bar No. 182260)
Allison S. Elgart (State Bar No. 241901)
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008

Interim Class Counsel for MCI Class

Ronald L. Motley
Jodi W. Flowers
Donald A. Migliori
Justin B. Kaplan
Vincent I. Parrett (State Bar No. 237563)
MOTLEY RICE, LLC
28 Bridgeside Boulevard
P.O. Box 1792
Mount Pleasant, SC 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9440

Interim Class Counsel For Verizon Class

Pursuant to General Order 45, Part X-B, the filer attests that concurrence in the filing of this document has been obtained from Vincent I. Parrett.[49]

49

Although not counsel of record for Plaintiffs in the Master Complaint, Plaintiffs wish to acknowledge the substantial contributions of the Electronic Frontier Foundation, the American Civil Liberties Union Foundation of Northern California, and the ACLU of Southern California to the preparation of this brief.